PALACKÝ UNIVERSITY OLOMOUC

Faculty of Science

Department of Optics and Optoelectronics

Entanglement-based continuous-variable quantum key distribution in realistic environment.

Master thesis

Author:	**Bc. Riabyi Pavlo**
Study programm:	**N1701/Physics**
Field of study:	**1701T029/ Optics and Optoelectronics**
Form of study:	**Present**
Supervisor:	**Dr. Vladyslav Usenko**
Deadline:	**26.04.2013**

„ I declare that this submitted thesis was worked out individually using referenced literature “.

In Olomouc, …………………...   ………………………………..

ACKNOWLEDGMENTS

First of all, I would like to express gratitude to my supervisor Dr. Vladyslav Usenko, who introduced me to quantum cryptography. His valuable suggestions and comments were extremely helpful during the entire time of study.

I am very grateful to employees of the department for the atmosphere which reigned on the faculty. It was real pleasure to learn and take experience with excellent teachers, employees, students. In particular, I thank prof. Dr. Zdenek Hradil, Dr. Jaromir Fiurasek, Dr. Radim Filip.

I would also like to thank prof. Dr. Oleh Angelsky for the opportunity to study and gain experience abroad. I am grateful to Claudia Zenkova for the support and also all employees of Engineering and Technical Faculty of a Yuriy Fedkovych Chernivtsi National University.

Last but not least, I would like to thank my parents and family for their support during all this time, without them it would be impossible to complete or even start the work. I would also like to thank all my friends for their support.

Bibliografická identifikace:

Jméno a příjmení autora	Bc. Riabyi Pavlo
Název práce	Kvantová distribuce klíče se spojitými proměnnými na základě kvantového provázání v realistickém prostředí.
Typ práce	Diplomová
Pracoviště	Univeryita Palackeho v Olomouci
Vedoucí práce	Vladyslav Usenko, Ph.D.
Rok obhajoby práce	2013
Abstrakt	Cílem práci bylo zkoumání protokolu kvantové kryptografie se spojitými proměnnými na základě kvantového provázání v podmínkách realistických nedůvěryhodných kanálů. Vliv fluktuace propustnosti kanálů ve volném prostoru na protokol na základě kvantového provázání byl studován a prokol byl ukázán pevnější proti fluktuace kanálu než protokol na základě koherentních stavů. Byl určen únik informací z obou provázaných modů, což odpovídá použití provázaného zdroje jako důvěryhodné střední stanice, s ohledem na realistické efekty atmosférických kanálů. Byla stanovena optimální poloha zdroje provázaných stavů v kanálu.
Klíčová slova	kvantová kryptografie, atmosférický kanál, key rate, fluktuace propustnosti, vzájemná informace, stlačené stavy, koherentní stavy, spojité proměnné, realistickém prostředí
Počet stran	51
Počet příloh	0
Jazyk	Anglický

Bibliographical identification:

Autor’s first name and surname	Bc. Riabyi Pavlo
Title	Entanglement-based continuous-variable quantum key distribution in realistic environment.
Type of thesis	Master
Department	Palacky University of Olomouc
Supervisor	Vladyslav Usenko, Ph.D.
The year of presentation	2013
Abstract	The goal of the project was the examination of the entangled-based continuous-variable quantum key distribution protocol in the conditions of realistic untrusted channels. The influence of fluctuating free-space channels on the protocol was studied and protocol based on entangled states was shown more robust against channel fluctuations than the one based on coherent states. Also, information leakage from the both entangled modes was considered, corresponding to the entangled source used as a trusted middle station, in conditions of realistic atmospheric channels. The optimal position of the source in the channel was determined.
Keywords	quantum cryptography, atmospheric channel, key rate, transmittance variance, mutual information, squeezed states, coherent states, continuous variables, realistic environment
Number of pages	51
Number of appendices	0
Language	English

PREFACE

In this work, study was conducted on entanglement-based continuous-variable quantum key distribution (CV QKD) in realistic environment. We considered information loss and took atmospheric effects of a realistic channel into account. Protocols stability was estimated in terms of maximum variance of the transmittance that has a direct impact on the key rate. Also, we investigated and determined the optimal location of the entangled source in the channel with fluctuations.

The work is a contribution towards of development of secure quantum networks based on the free-space channels.

CONTENTS

INTRODUCTION

We live in times when a person interacts with flow of information. This is the Internet, mobile communications, electronic payment systems, which until recently seemed just the prospect of the future. And today we can see that they have become an integral part of our daily lives.

Clearly, all this information must be protected. To solve this problem the science of cryptography was developed. It deals with privacy (impossibility to read information from outside) and authentication (integrity and authenticity of authorship, and the impossibility of non-attribution) of access to information. Typically modern cryptography is using open encryption algorithms that involve the use of computational tools. There are more than a dozen encryption algorithms that, using the key of sufficient length and correct implementation of the algorithm, provide enciphering of text. In particular encryption algorithms such as Twofish, IDEA, and RC4 are widely used. They are based mostly on computational complexity. At the moment this is more than enough, but the prospect of creating a quantum computer [1] that will run many orders of magnitude faster than conventional classical computers can bring the whole defense based on classical cryptography to zero. In particular, one of the typical tasks for a quantum computer is factorization of on integer number by the product of prime factors, which is solved by the quantum Shor algorithm [2].

This gave rise to a more active research in the field of quantum cryptography, which security method is based on the principles of quantum physics. The technology of quantum cryptography relies on the uncertainty principle of quantum behavior of the system - it is impossible to precisely measure both position and momentum of a particle, also it is impossible to measure one parameter of a photon without distorting other. This is a fundamental property of nature, which in physics is known as the Heisenberg uncertainty principle, formulated in 1927. In view of these facts it is safe to say that quantum cryptography is the solution for the issue of security of communications both currently and in the future.

Nevertheless, it requires study and improvement, particularly taking into account realistic conditions. Therefore in this work we study the impact of fluctuations in atmospheric transmission channels on one of the modern quantum cryptography protocols.

CHAPTER I

Introduction and History of Classical Cryptography and classical theory of information

Cryptography (from Greek *kryptós* - hidden and *gráphein* - write) - the study of mathematical methods for providing privacy (impossibility to read information from outside) and authentication (integrity and authenticity of authorship) of information [3]. Developed from the practical need to transmit important information most effectively. For mathematical analysis cryptography uses tools of abstract algebra.

For a long time cryptography was understood only as *encryption* - the process of converting ordinary information (plaintext) into senseless "garbage" (encrypted text). *Decryption* - a reverse process for retrieval of encrypted text. Cipher is a pair of algorithms used for encryption /decryption. Key - a secret code (ideally known only to two parties) for a particular context while transmitting the message. The keys are of great importance.

History of cryptography. So far, cryptography dealt solely with private messages (i.e. encryption) - conversion of messages from a comprehensible form into an incomprehensible and reverse recovery on the receiver side, making it impossible to read for someone who overheard or intercepted without secret knowledge (namely the key needed for message decryption). In recent decades, the scope of cryptography has expanded to include not only the transmission of secret messages, but also methods for checking the integrity of messages, identify the sender / recipient (authentication), digital signatures, interactive confirmation and secure communication technology, and more.

The earliest forms of cryptography require no more than a and paper, because in those days most people could not read. With the spread of literacy, the need in cryptography appeared. The main types of classical ciphers are permutation codes that change the order of the letters in the message, and substitution ciphers, which systematically replace letters or groups of letters by other letters or groups of letters. Simple variations of both types offered little protection from experienced opponents. One of the earliest was substitution at Caesar’s cipher in which each letter is replaced by a letter a different position in the alphabet. This cipher was named after Julius Caesar, who used it, with a shift in the 3 position to communicate with the generals in military campaigns.

Cipher text obtained from classical cipher; always give some statistical information about the text messages that can be used to break. The security after the discovery of frequency analysis in the 9 century, nearly all such ciphers became more or less easily breakable. Classical ciphers retained popularity, mainly in the form of puzzles. Almost all ciphers remained vulnerable to cryptanalysis using the frequency analysis.

Various mechanical devices and tools were to aid in encryption. One of the first is “skitala” in ancient Greece, reed, which is believed to be the Spartans used as a permutation cipher. Some mechanical encryption / descramble devices were created in the early 20th century, many patented, in particular rotor machines - the most famous among them is Enigma, machine, used in the World War II. The emergence of digital computers and electronics after WWII made possible the development of more complex ciphers. Moreover, computers allow one to encrypt any data that can be represented in binary form, unlike classical ciphers which were developed for encryption of written texts. This made it unsuitable to use linguistic approaches in cryptanalysis. Many computer ciphers can be characterized by their work with sequences of binary bits, unlike classical and mechanical schemes which usually work directly with the letters. However, computers have also found applications in cryptanalysis, which, to some extent, offset the increasing complexity of the ciphers. Nonetheless, good modern ciphers stayed ahead of cryptanalysis, typically the use of high-quality cipher is very efficient, while the scrapping of these codes requires much more effort than before, making cryptanalysis so inefficient and impractical that break is almost impossible.

Extensive academic research in cryptography emerged relatively recently - since the mid-1970s, with the advent of open specification standard DES (Data Encryption Standard) from U.S. National Bureau of Standards. Since then, cryptography has become a widespread instrument for data security in computer networks and information security in general. The current level of security of many cryptographic techniques is based on the complexity of some computational problems, such as the factorization of integers, or problems with discrete logarithms. In many cases, there is evidence of safety cryptographic techniques only if it is impossible to effectively solve a computational problem.

By the early 20th century, cryptography mainly been associated with linguistic schemes. Once the emphasis shifted, cryptography is extensively using mathematical tools, including information theory, computational complexity, statistics, combinatorics, abstract algebra and number theory. Cryptography is also a branch of engineering, but not common because it deals with active, intelligent and resourceful enemy

1.1 Types of encryption

Speaking of encryption cryptography is currently distinguished between ***symmetric*** and ***asymmetric*** encryption.

Algorithms for ***symmetric encryption*** include encryption methods in which both the sender and recipient of messages use the same key.

Recent studies of symmetric encryption algorithms centered on the block and stream encryption algorithms and their applications. Block ciphers use a piece of plaintext and key, and produce the output cipher text of the same size. Because the messages are usually longer than one block, some method of bonding consecutive blocks must be used. Several methods have been developed that differ in various aspects.

Ciphers such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [4] are the standard block ciphers approved by the U.S. government. Despite the fact that the standard DES was considered obsolete, it is still quite popular and is used in many cases, from ATM encryption to the privacy of emails and secure access to remote terminals.

Stream ciphers, in contrast to the block, create a key of arbitrary length, imposed on the plaintext bit-wise. In stream cipher, cipher text stream is calculated based on the internal state of the algorithm, which varies during its operation. RC4 is an example of a well-known and widespread stream cipher [4].

Cryptographic hash functions do not necessarily use the key, but are often used and are an important class of cryptographic algorithms. These functions take data and calculate short fixed-size number.

Message authentication codes (MAC) are similar to cryptographic hash functions, except that they use the secret key for authentication hash value. These features offer protection against attacks on ordinary hash function.

Unlike symmetric, ***asymmetric encryption algorithms*** use a pair of related keys - public and private. Thus, despite the connectivity of open and secret key in the pair, computing the private key from public is considered technically impossible.

In asymmetric cryptosystems, the public key can be freely distributed, while the private key is kept secret. Typically, the public key is used for encryption, while the private (secret) key is used for decryption.

1.2 The concept of key in cryptography

Key - a certain value, which working in conjunction with the algorithm makes a certain cipher text. In asymmetric cryptography, the bigger the key, the more secure resulting cipher text is. However, the size of the asymmetric key and symmetric secret key size is comparable. Symmetric 80-bit key is equivalent to the stability of 1024-bit public key. Symmetric 128-bit key is approximately 3000-bit public. Again, the more the higher reliability, but the mechanisms underlying each type of cryptography are quite different, and comparing their keys in absolute terms is irrational.

Despite the fact that the key pairs are mathematically related, it is almost impossible to calculate the public key from the secret one, at the same time, the calculation of the private key is always possible by having available sufficient time and computing power. That is why it is vital to create the correct key length: big enough to be reliable, but small enough to remain fast at work.

According to modern concepts 128-bit symmetric keys are quite robust and not subject to cracking, at least for as long as someone does not build a functioning quantum supercomputer. 256-bit keys according to cryptographers cannot be broken even in theory, and even on a hypothetical quantum computer. For this reason, the algorithm AES supports key length of 128 and 256 bits. But history teaches us that all these assurances in decades may be empty chatter. The only system which has been proven secure (1949) Shannon [5], is a one-time pad system by Vernam.

One-time pad system by Vernam(Vernam cipher) was invented in 1917 and was mathematically proven secure. It works for the cipher text plaintext combined using operation "XOR" with the key (called a one-time pad). In this case, the key is to have three crucial properties:

- be truly random
- coincide in size to specify the plaintext
- used only once

This is based on the idea cipher pad: cryptologist in person is provided with a notebook, each page of which contains the key. The same notepad is at the receiving side. Used pages are destroyed. In addition, if there are two independent channels, each of which is low probability of intercept, but not zero, time pad cipher is also useful: one channel can transmit an encrypted message, the other - the key. In order to decrypt the message, the interceptor must listen to both channels. Vernam cipher can be used if there is a one-way encrypted channel: the key is transmitted in one direction under the protection of the channel messages to the other side of the protected key.

The disadvantages of this system are:

- sensitive to any violation of the encryption process
- there may be problems with the reliable disposal of used pages
- problem is the secure transmission sequence and store it in secret
- necessity of truly random sequence (key)
- if a third party somehow finds out a message, it is easy to recover the key and will be able to substitute a message to another of the same length.

The above mentioned disadvantages can by the use of key distribution schemes, such as quantum cryptography.

1.3 Classical information theory

The term information was used extensively in the scientific literature since the 30s-40s of the twentieth century. In 1948, investigating the problem of efficient transmission of information through a noisy communication channel, Claude Shannon proposed a revolutionary probabilistic approach to the understanding of communication and created the first, truly mathematical, theory of entropy [6]. His sensational ideas quickly formed the basis for the development of two main areas: information theory, using the concept of probability and ergodic theory to study the statistical characteristics of data and communication systems, and coding theory, which uses mainly algebraic and geometric tools to develop effective codes. So it appeared the famous Shannon entropy [7], a measure of uncertainty or unpredictability information, which is given by:

$$H(X)=-\sum_{x\in X} p(x) \log p(x) \tag{1.1}$$

Let's consider the two-sided source consisting of correlated pairs, denoted by letters (X, Y) with distribution $p(x,y)$, which are possessed by Alice (X) and Bob (Y) (Figure 1).

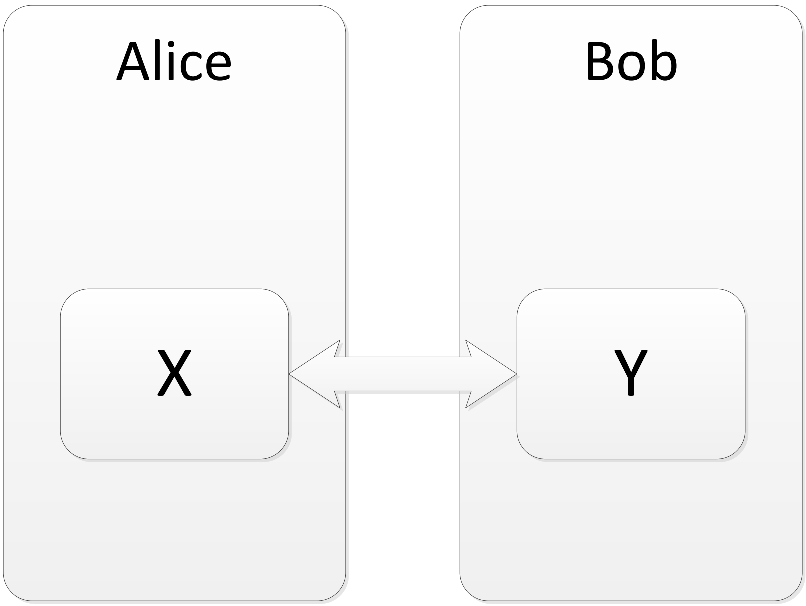

Figure 1

The joint entropy H (X, Y) of a pair of discrete random variables (X, Y) with alphabets X = {0,1, ... d1} and Y = {0,1, ... d2} with joint distribution $p(x,y)$ is defined as:

$$H(X ,Y)= -\sum_{x\in X}\sum_{y\in Y} p(x,y) \ \log p(x,y) \tag{1.2}$$

Unlike normal entropy H (X), joint entropy H (X, Y) has the interpretation of uncertainty about the pair (X, Y).

The conditional entropy H (Y | X) of pair of discrete random variables (X, Y) with a joint distribution p (x, y) is defined as:

$$\text{H (Y|X)}= \sum_{x\in X} p(x)H\ (Y|X = x) \qquad (1.3)$$

$$\text{H (Y|X)}= -\sum_{x\in X} \sum_{y\in Y} p(x, y)\ \log p(y|x) \qquad (1.4)$$

The conditional entropy H (Y | X) is the interpretation of uncertainty in Y, if we know X. Both joint and conditional entropy connected by chain rule can be graphically represented using Winn diagram, as shown in Figure 2.

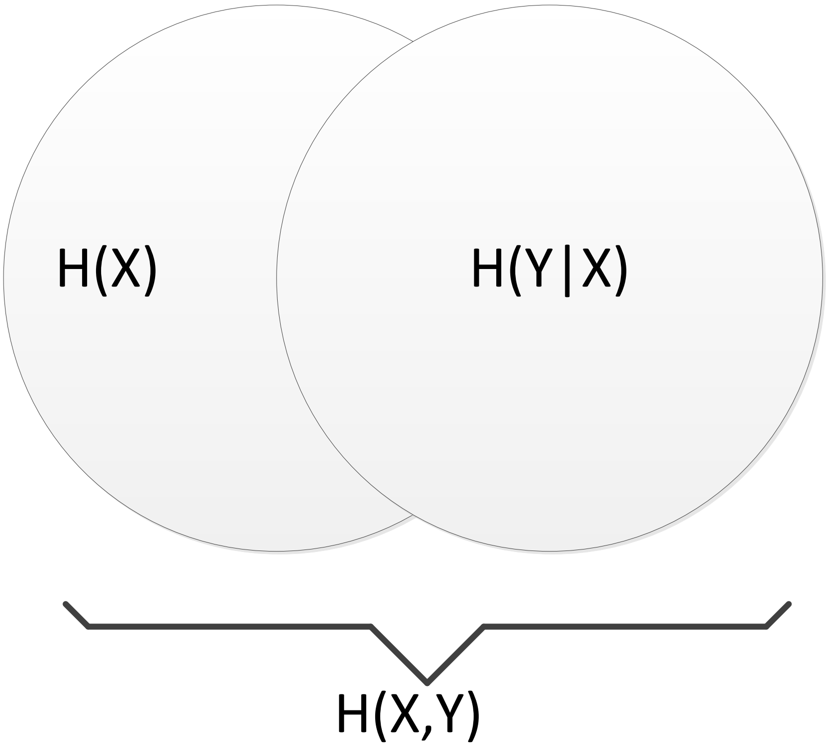

Figure 2

The mutual information H (X: Y) of a pair of discrete random variables (X, Y) is represented by the expression:

$$\text{H (X:Y)}= -\sum_{(x,y)\in X*Y} p\ (x, y) \log \frac{p\ (x,y)}{p\ (x)p(y)} \qquad (1.5)$$

The mutual entropy (or mutual information) H (X: Y) with bilateral sources (X, Y) is interpreted as the number of correlations between Alice and Bob, and is measured in bits of correlation. Using the definition of mutual information, conditional entropy and entropy can get the following relationship:

$$H\ (X:Y)= H\ (X)+ H\ (Y)- H\ (X,Y) \tag{1.6}$$

The relationship between H (X), H (Y | X), H (X | Y) and H (X: Y) can be obtained by Winn diagram (Figure 3)

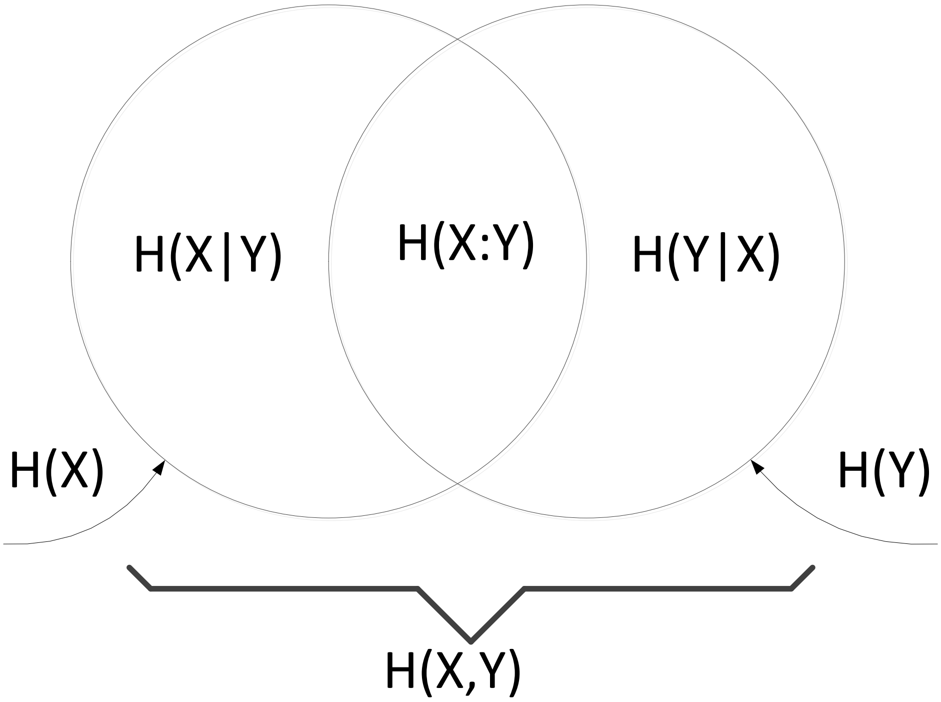

Figure 3

Let's consider the important case of Gaussian distributions that will be used later in the work. First we consider the normal distribution with variance V_x:

$$g(x)= \frac{1}{\sqrt{2\pi V_x}}\, e^{\frac{-x^2}{2V_x}} \tag{1.7}$$

The expression for the differential entropy, which corresponds to a continuous distribution, can be written as:

$$H\ (X)= \frac{1}{2}\log V_x + C \tag{1.8}$$

where C is an arbitrary constant, associated with scaling.

For bipartite normal Gaussian distribution with covariance matrix:

$$\mathrm{K_{AB}} = \begin{bmatrix} \langle x^2 \rangle & \langle xy \rangle \\ \langle xy \rangle & \langle x^2 \rangle \end{bmatrix} \qquad (1.9)$$

differential entropy can be written as:

$$\mathrm{H(X,Y)} = \frac{1}{2}\log(\det\mathrm{K_{AB}}) + \mathrm{C'} \qquad (1.10)$$

The conditional entropy H (Y | X) of distribution of Y under fixed X can be written as:

$$\mathrm{H(Y|X)} = \frac{1}{2}\log \mathrm{V_{Y|X}} + \mathrm{C} \qquad (1.11)$$

where $\mathrm{V_{Y|X}}$ is the variance of Y, where X is known, and is written as follows:

$$\mathrm{V_{Y|X}} = \frac{\det\mathrm{K_{AB}}}{\mathrm{V_x}} = \langle y^2 \rangle - \frac{\langle xy \rangle^2}{\langle x^2 \rangle} \qquad (1.12)$$

Mutual entropy (mutual information) of a bipartite distribution has three equivalent definitions:

$$\mathrm{H\ (X{:}Y)} = \frac{1}{2}\log\left[\frac{\mathrm{V_Y}}{\mathrm{V_{Y|X}}}\right] \qquad (1.13)$$

$$\mathrm{H\ (X{:}Y)} = \frac{1}{2}\log\left[\frac{\mathrm{V_X}}{\mathrm{V_{X|Y}}}\right] \qquad (1.14)$$

$$\mathrm{H\ (X{:}Y)} = \frac{1}{2}\log\left[\frac{\mathrm{V_{X|Y}}}{\det\mathrm{K_{AB}}}\right] \qquad (1.15)$$

CHAPTER II

Introduction to quantum cryptography

Along with classical cryptography, in recent decades quantum cryptography was rapidly developing. This science originated in 1984, when the first quantum key distribution protocol, named BB84 was developed [8]. In fact, quantum cryptography deals with of the key transfer, such key is then used in the system of one-time pad. The main advantage of quantum cryptographic protocols compared to classical is a serious theoretical study of their stability: in classical cryptography security is reduced, usually by assumptions about computational capabilities of the attacker, the quantum cryptography interceptor can enjoy all actions permissible by the laws of nature, and still he cannot know the secret key without being noticed.

An important feature for quantum cryptography is the property collapse of the wave function in quantum mechanics, which means that with the measurement of the quantum-mechanical system, its initial state reduces. This property is used to justify quantum cryptography: when trying to eavesdrop on a key interceptor inevitably makes a mistake, causing it to be detected by additional noise on the receiving side. Therefore, the decision about the possibility of secret key distribution achieved by legitimate users is based on the value of observational errors on the receiving side: when rate of the errors approaches the critical value (depending on the protocol) secret key length in bits tends to zero, and transfer of key is impossible.

This means that the most important characteristic of quantum cryptography protocols are permissible fatal error at the receiving end, for which possible dissemination of secret keys is possible: the greater it is, the more stable is the system of quantum cryptography against intrinsic noise and eavesdropping attempts. An important result is the determination of the exact value of the critical errors for BB84 protocol, which is equal to about 11% [9-11].

Experimental realization of quantum cryptography came across a number of technological challenges, the most important of which is the difficulty of generating strictly single-photon quantum states. In practice attenuated laser pulses are commonly used which are described as coherent quantum states. Laser radiation has a Poisson distribution for the number of photons, so with a certain probability that depends on the average number of photons in the coherent states can occur an event, where there are two, three or more photons in a pulse with diminishing probabilities. This is an important assumption, since the use of multiphoton states, combined with the inevitable attenuating channels, provides the possibility for an eavesdropper to delay the photons, and measure them after getting some information from legitimate users, which is transmitted over a public channel, resulting in quantum cryptography schemes to lose their privacy. Such actions are called PNS-attacks (Photon number splitting attack). Developments in the field of anti-PNS-attack led to the novel protocols (compared with BB84). Such development provides key generation, no longer allowing interceptors get all the information about the key, even with successful delay of the transmitted photons in their quantum memory. One of the protocols resistant to PNS-attack is a protocol SARG04, proposed in 2004. The analysis revealed that it ceases to be secret only when the interceptor is able to block the entire one-, two-and three photons in a pulse. This means that the distribution of quantum keys is possible on larger distances than using protocol BB84 since possible length of secure channel depends on the average number of photons in the pulse. Thus, we can talk about the concept of critical distance for distribution of secret keys, in which part of the pulse with a large number of photons is small, and security against PNS attacks determines precisely this critical distance.

2.1 The concept of states

Wave function and clean condition. State of particle (or system of particles, if there are many) is represented in quantum mechanics by the *wave function* - an object for description of quantum picture of the world. We first introduce the notion of a pure quantum state, which is a vector in Hilbert space ***H***:

$$\|\psi\| = \sqrt{(\psi,\psi)}, \qquad \psi \in \mathrm{H} \tag{2.1}$$

In quantum information theory notation introduced by Dirac is commonly used for states and operators. State of ψ is denoted as $|\psi\rangle$ and conjugate state$\langle\psi|$. Then the scalar product of vectors ψ^* and ψ is written as$\langle\psi|\psi\rangle$.

For each pure quantum state $|\psi\rangle$ can define the corresponding operator $\rho_\psi = |\psi\rangle\langle\psi|$, which is called the density operator. This operator has rank 1, it should be equal to one and it acts as a projection of a state$|\psi\rangle$.

Mixed states. Mixed quantum state is a statistical mixture of several pure states (i.e. the set of pure states with corresponding probabilities):

$$\rho = \sum_{\mathrm{i}} \rho_{\mathrm{i}}\, |\psi_{\mathrm{i}}\rangle\langle\psi_{\mathrm{i}}|, \;\; \rho_{\mathrm{i}} \geq 0 \;\; \forall \mathrm{i}, \;\; \sum_{\mathrm{i}} \rho_{\mathrm{i}} = 1 \tag{2.2}$$

It is also a positive definite:

$$\langle\varphi|\rho|\varphi\rangle = \sum_{\mathrm{i}} \rho_{\mathrm{i}}\, |\, \langle\varphi|\psi\rangle|^2 \geq 0 \qquad \forall\, |\varphi\rangle \in \mathrm{H} \tag{2.3}$$

Further, any Hermitian operator A has the spectral decomposition, which is:

$$\mathrm{A}{=}\sum_{\mathrm{i}} \lambda_{\mathrm{i}}\, |\lambda_{\mathrm{i}}\rangle\langle\lambda_{\mathrm{i}}| \tag{2.4}$$

with eigenvalues λ_{i} and eigenvectors $|\lambda_{\mathrm{i}}\rangle$. This means that any positive Hermitian operator with unit trace can be called the density operator of a quantum state: the positive definiteness implies positivity of all eigenvalues (which are treated as probabilistic weights). This leads to a general definition of quantum state: Quantum state - positive Hermitian operator in Hilbert space H with unit trace.

2.2 Multipartite and entangled

Consideration of quantum systems consisting of several parts (components of systems) can sometimes lead to interesting properties that are not found in the classical case. In 1935, in correspondence of Einstein, Podolsky and Rosen [12] were observed very unusual properties of quantum systems components that are contrary locality: it turned out that the actions of one of the subsystems can instantly affect another subsystem, no matter what is the distance between them. Description of this property has led to the emergence of the formalism of quantum systems components.

In the most elementary case of two qubits the entangled state (called EPR) can be written as a superposition:

$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.5}$$

Consider the state of the EPR pair in the space of two qubits, and conduct measurement on the first subsystem. The initial state collapses into a pure state $|00\rangle$. Similarly, when receiving the result 1, the initial state is converted into $|11\rangle$. This suggests a surprising fact: only one measurement of a quantum state can capture the whole situation in general.

The said property is not valid for arbitrary quantum states, but only for their important class called entangled states. They are defined as states on the combined state space that cannot be represented as a tensor product of states in each partial space:

$$\rho_{12} \neq \rho_1 \otimes \rho_2 \tag{2.6}$$

For states that are not entangled, such property does not hold: measurement on one subsystem does not affect the other.

2.3 Impossibility of cloning

One can consider another partial result from the quantum theory that is important for quantum cryptography. Non-orthogonal quantum states cannot be reliably distinguished, and unknown states cannot be cloned; for example, in order to gather more complete statistics of measurement results. The transformation U, which clones an arbitrary pure quantum state $|\psi\rangle$, can be described as follows:

$$\mathrm{U}|\psi\rangle\otimes|\mathrm{A}\rangle=|\psi\rangle \otimes |\psi\rangle \tag{2.7}$$

where $|\mathrm{A}\rangle$ - supporting input state of the system.

In order to show the impossibility of such a transformation, let's consider its action on the basis states $|0\rangle$ i $|1\rangle$

$$\mathrm{U}|0\rangle\otimes|\mathrm{A}\rangle=|0\rangle \otimes |0\rangle \tag{2.8}$$

$$\mathrm{U}|1\rangle\otimes|\mathrm{A}\rangle=|1\rangle \otimes |1\rangle \tag{2.9}$$

and the state $\frac{1}{\sqrt{2}}(|0\rangle +|1\rangle)$. Due to the linearity of the operator U, the above equations must be made:

$$\mathrm{U}\,(\tfrac{1}{\sqrt{2}}(|0\rangle +|1\rangle))\otimes|\mathrm{A}\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle \otimes|0\rangle + |1\rangle \otimes|1\rangle) \tag{2.10}$$

On the other hand from the definition of U must come:

$$\mathrm{U}\,(\tfrac{1}{\sqrt{2}}(|0\rangle +|1\rangle))\otimes|\mathrm{A}\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle \otimes|1\rangle + |0\rangle \otimes|1\rangle) \tag{2.11}$$

The resulting contradiction proves the impossibility of cloning [13, 14] arbitrary quantum states.

2.4 Continuous variables

The system of continuous variables [15] is canonical to infinite-dimensional quantum system consisting of N modes, which is described in the Hilbert space as a result of the tensor product of N infinite Fock spaces χ_i. One could assume N modes of the electromagnetic field, where mode can be with different frequencies ω_i, polarization and spatial location. Then χ_i is the set of Fock bases $\{|n\rangle_k\}$ of eigenvalues of the operator $\hat{n}_i = \hat{a}_i^{\dagger}\hat{a}_i$. Vacuum state on general Hilbert space is written as $|0\rangle = \otimes_i |0\rangle_i$, where $\hat{a}_i|0\rangle_i$=0, is the ground state of a system of N harmonic oscillators that is described by Hamiltonian without interaction:

$$H=\sum_{i=1}^{N}\left[\hat{a}_i^{\dagger}\hat{a}_i + \frac{1}{2}\right] \tag{2.12}$$

where $\hat{a}_i^{\dagger}$ i $\hat{a}_i$ are annihilation and creation operators of mode "i" satisfying the bosonic commutation relations:

$$\left[\hat{a}_i\hat{a}_j^{\dagger}\right] = \delta_{ij}, \left[\hat{a}_i\hat{a}_j\right] = \left[\hat{a}_i^{\dagger}\hat{a}_j^{\dagger}\right] = 0 \tag{2.13}$$

The corresponding quadrature operators that are analogues coordinate and momentum operators for each mode is defined as:

$$\hat{x} = (\hat{a}^{\dagger} + \hat{a}) \tag{2.14}$$

$$\hat{p} = (\hat{a}^{\dagger} - \hat{a}) \tag{2.15}$$

The quadratures can be grouped into a vector:

$$\hat{r} = (\hat{r}_1, \dots, \hat{r}_{1N})^T = (\hat{x}_1, \hat{r}_1, \hat{x}_2, \hat{r}_2, \dots, \hat{x}_N, \hat{r}_N,)^T \tag{2.16}$$

which can be written in a compact form bosonic canonical commutation relations between operators quadrature:

$$[\hat{r}_k, \hat{r}_l] = i\Omega_{kl} \tag{2.17}$$

where Ω is symplectic form:

$$\Omega = \otimes_{i=1}^{N}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{2.18}$$

The probability distribution function for quadratures, the Wigner function, which can be written as follows in term of the eigenvectors of the quadrature operators, looks like:

$$W(x,p) = \frac{1}{(2\pi)^N} \int \langle x - x'|\rho|x + x'\rangle \, x^{ix'*p} \, d^N x' \, , \quad x,p \; \in R^N \qquad (2.19)$$

Gaussian states of light which we work with are described by the Gaussian Wigner function which reads:

$$W(r) = \frac{1}{\pi^{2N}\sqrt{det\gamma}} e^{-(r-d)^T \gamma^{-1} (r-d)} \qquad (2.20)$$

where d are the displacement vector ($d \in R^{2N}$) and the positive-semidefinite symmetric 2N × 2N covariance matrix γ, which reads as:

$$\gamma_{ij} = Tr[\rho\{(\hat{\mathrm{r}}_{\mathrm{i}} - d_i), \left(\hat{\mathrm{r}}_{\mathrm{j}} - d_j\right)\}] \qquad (2.21)$$

here d, for a general density operator ρ, can be written as:

$$d = \langle \hat{\mathrm{r}} \rangle = Tr[\rho \hat{\mathrm{r}}] \qquad (2.22)$$

In general, in probability theory and statistics, a **covariance matrix** is a matrix, whose element in the i, j position is the covariance between the elements of a random vector. The covariance matrix of the random vector is a square symmetric matrix, which are located on the diagonal components of variance, and the off-diagonal elements - covariance between the components.

Coherent and squeezed states. In 1926, Schrödinger considered the motion of Gaussian wave packets represent as harmonic oscillators. As it turned out, the wave function of states does not change its shape with time and minimizes uncertainty relation. These two properties suggest these states are closest to the classical. So the concept of coherent states was introduced in quantum mechanics, and become one of the main tools of quantum optics.

Coherent states $|\alpha\rangle$ are eigenstates of the annihilation operator, corresponding to the complex number α:

$$\hat{\alpha}|\alpha\rangle = \alpha|\alpha\rangle \tag{2.23}$$

Parameters α set for coherent states mean values of quadrature (which be described later) (Figure 4):

$$\langle x\rangle = \sqrt{2}\mathrm{Re}\alpha \tag{2.24}$$

$$\langle p\rangle = \sqrt{2}\mathrm{Im}\alpha \tag{2.25}$$

Coherent states can be regarded as vacuum states that are shifted in phase space.

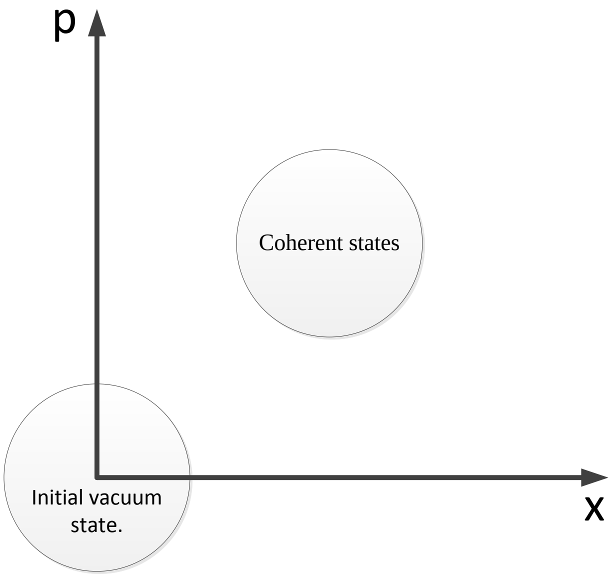

Figure 4

For such states the uncertainty relation is:

$$\langle \Delta x^2\rangle\langle \Delta p^2\rangle = 1 \tag{2.26}$$

If we consider the **squeezed state** (Figure 5), in which compression is one of the quadratures respectively, as shown in Figure:

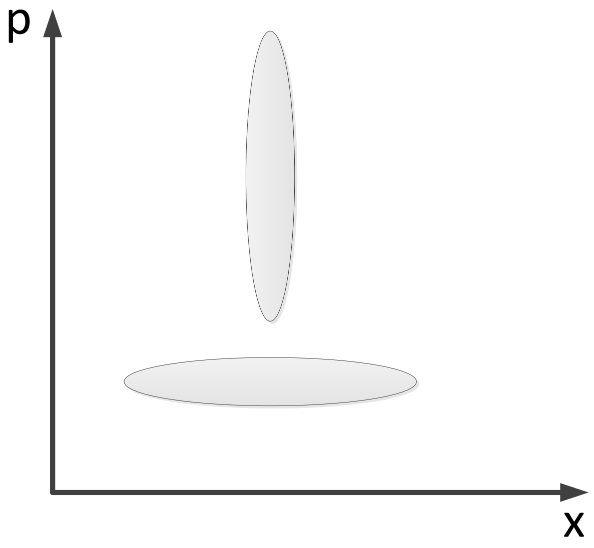

Figure 5

If we overlay modulated squeezed states in orthogonal quadratures, we get form of the thermal state (Figure 6).

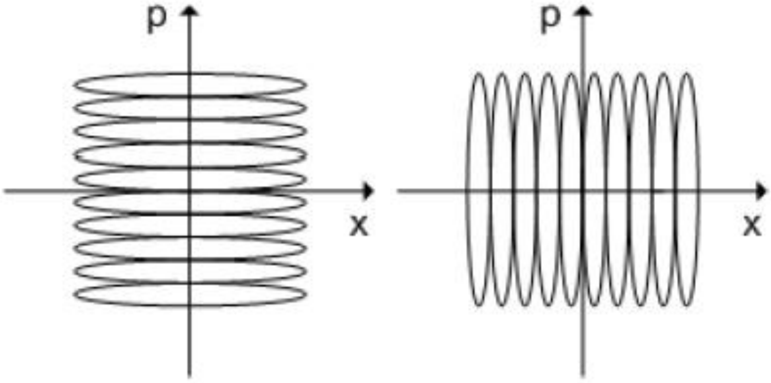

Figure 6

The effect of the squeezing operation is better understood using the

quadratures description of the electromagnetic field. The Hamiltonian can be written:

$$H = \frac{i}{2}[\hat{x}\hat{p} + \hat{p}\hat{x}] \tag{2.27}$$

this together with the Heisenberg equation of motion gives the quadratures transformation:

$$\begin{bmatrix} \hat{\mathrm{x}} \\ \hat{\mathrm{p}} \end{bmatrix}_{out} = \begin{bmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{bmatrix} \begin{bmatrix} \hat{\mathrm{x}} \\ \hat{\mathrm{p}} \end{bmatrix}_{in} \tag{2.28}$$

where $r = \tau\Delta t$, and τ is the squeezing parameter related to the intensity of the pump laser and the strength of the non-linear interaction and φ corresponds to a phase rotation.

2.5 Measurement in quantum optics

The most important difference from classical theory is that, in general, the measurement of a quantum system modifies its original state. In quantum optics we consider two types of measurement, those that resolve the photon number states and those which measure the quadratures of the field.

In the first case, for the measurement of photon numbers the avalanche photodiodes (APD) are used, which are tuned to sense a single photon, which is already technically very challenging.

In the second case, for the measurement the quadratures of the electromagnetic field the so-called homodyne detection is used, which is shown in Figure 7:

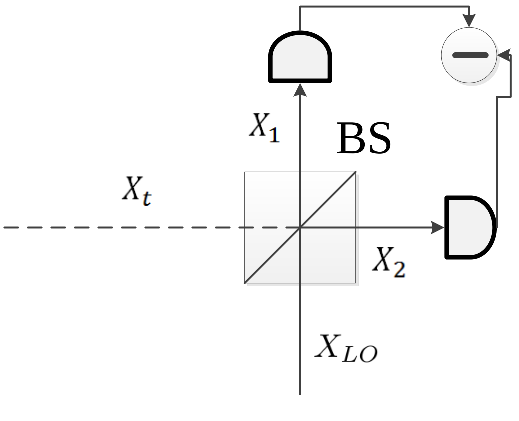

Figure 7

On the picture can be seen the incoming mode X_t, which combined with the local oscillator X_{LO} on a balanced beamsplitter, after which we obtain the outgoing modes X_1 and X_2:

$$\hat{x}_1 = \frac{\hat{x}_t + X_{LO}}{\sqrt{2}}; \quad \hat{p}_1 = \frac{\hat{p}_t}{\sqrt{2}} \tag{2.29}$$

$$\hat{x}_2 = \frac{\hat{x}_t - X_{LO}}{\sqrt{2}}; \quad \hat{p}_2 = \frac{\hat{p}_t}{\sqrt{2}} \tag{2.30}$$

The intensity of the outgoing modes are measured with two photodetectors, which after subtraction give a signal proportional to the measured quadrature $\hat{x}_t$.

CHAPTER III

The protocols of quantum cryptography

3.1 Protocol BB84

In 1984 the basic principles of quantum cryptography were developed along with the arguments in favor of secrecy of this method of key distribution. Then it was time for the development of the formalism of quantum cryptography: the necessary actions for legitimate users to detect the interceptor were formalized and the secrecy of the first quantum key distribution protocol, named BB84, was proved.

The general scheme of the protocol. Informally principle of all protocols of quantum cryptography can be described as follows: transmitting party (Alice) at each step sends one of the states, prepared in one of the basis and the receiving party (Bob) carries a measurement, so that after additional exchange of classical information between the parties they should have bit strings that are identical in the case of perfect channel and no interceptor. Errors in these lines can speak about no-ideal channel and the actions of the attacker. When the value of error exceeds a certain limit, the protocol is interrupted, otherwise legitimate users can obtain completely secret key from their (partial correlated) bit strings.

Transmission of signal states. BB84 protocol uses two basis:

$$+: \quad |x\rangle = |0\rangle, \qquad |y\rangle = |1\rangle \tag{3.1}$$

$$\times: \quad |u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |v\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{3.2}$$

At the stage of preparation of the states Alice randomly chooses one of these bases, then randomly chooses value of a bit:

- $|x\rangle$, if the basis "+" and the value of the bit is 0,
- $|y\rangle$ in the same basis and bit value of 1,

- $|u\rangle$ if the basis “×” and bit is 0,
- $|v\rangle$ if the basis “×” and bit is 0,

When sending each of these signals Alice remembers choice of basis and the bit values, which leads to appearance of two random bit strings on her side. Bob, getting the signals sent by Alice, carries over them randomly one of the two measurements, each of which is able to give reliable result due to orthogonality of the states inside all of basis of Alice:

$$\mathrm{M}_0^{+} = |\mathrm{x}\rangle\langle\mathrm{x}|, \mathrm{M}_1^{+} = |\mathrm{y}\rangle\langle\mathrm{y}| \quad (3.3)$$

$$\mathrm{M}_0^{\times} = |u\rangle\langle u|, \mathrm{M}_1^{\times} = |v\rangle\langle v| \quad (3.4)$$

As a result, he have two lines: with the bases settings, and the results of the measurements. Then the trusted parties apply additional classical error correction and privacy amplification algorithms and obtain a secure key.

3.2 Protocol E91

Protocol E91 by A. Ekert was proposed in 1991 [16]. The second name protocol - EPR, as it is based on the paradox of Einstein-Podolski-Rosen. The protocol is proposed to use, for example, a pair of photons, which are created in the antisymmetric polarization states. Interception one of the photons pair Eve does not bring any information, but it is for Alice and Bob signal that their conversation was eavesdropped.

EPR effect occurs when a spherically symmetric atom emits two photons in opposite directions toward the two observers. Photons are emitted with the uncertain polarization, but due to the symmetry the polarization is always opposed. An important feature of this effect is that the polarization of photons becomes known only after the measurement. Based on EPR Ekert proposed protocol which guarantees the security of key distribution. The sender generates a certain amount of EPR photon pairs. One photon from each pair he keeps for himself, the other sends to his partner. However, if the detection efficiency is close to unity, while the sender is getting polarization value of 1, his partner registers 0 and vice versa. Clearly, therefore partners whenever necessary may obtain identical random code sequences.

Originally created as N EPR-entangled photon pairs, then one photon from each pair is sent to Alice and the other - Bob. For these EPR-pairs, there are three possible quantum states:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \left|\frac{3\pi}{6}\right\rangle_B - \left|\frac{3\pi}{6}\right\rangle_A |0\rangle_B\right) \tag{3.5}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(\left|\frac{\pi}{6}\right\rangle_A \left|\frac{4\pi}{6}\right\rangle_B - \left|\frac{4\pi}{6}\right\rangle_A \left|\frac{\pi}{6}\right\rangle_B\right) \tag{3.6}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(\left|\frac{2\pi}{6}\right\rangle_A \left|\frac{5\pi}{6}\right\rangle_B - \left|\frac{5\pi}{6}\right\rangle_A \left|\frac{2\pi}{6}\right\rangle_B\right) \tag{3.7}$$

This can be written in the general form:

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}\left(|0_i\rangle_A |1_i\rangle_B - |1_i\rangle_A |0_i\rangle_B\right) \tag{3.8}$$

This formula shows that each of these three states are encoding bits "0" and "1" in a unique basis. Then Alice and Bob perform measurements on their parts of separated EPR-pairs by applying appropriate projectors:

$$P_1 = |0\rangle\langle 0|,\ P_2 = \left|\frac{\pi}{6}\right\rangle\left\langle\frac{\pi}{6}\right|,\ P_3 = \left|\frac{3\pi}{6}\right\rangle\left\langle\frac{3\pi}{6}\right| \tag{3.9}$$

Alice records the measured bits, and Bob writes them a supplement to 1. The results of measurements in which users choose the same bases form the key. Experiments with the implementation of this protocol started recently. Their performance was made possible after development of the sources of entangled pairs with a high degree of correlation and long lifetime.

To implement this protocol sources entangled pairs are used. They are based on the parametric non-linear crystals, in which the pump photon produces a pair of photons. The disadvantage of this scheme is a wide spectral range of photons, making them more sensitive to chromatic dispersion, which requires spectral filtering.

3.3 Protocols on continuous variables

Disadvantage that limits the effectiveness of quantum cryptography is that most measurements are not effective if strongly attenuated laser pulses are used. This encourages the creation of quantum cryptography protocols in which the majority of acts measurements were informative. This can be done using intense beams and continuous variables.

One of the first such protocols was developed by Hillery [17], who in 2000 proposed a scheme based on the application of light, and bits of key, which are encoded in the values of compressed quadrature of field. In this case, Alice randomly chooses which of quadrature is used to squeezing and encoding, as well as Bob randomly chooses which of the quadratures measure. In this protocol, as well as in the protocol based on discrete variables (eg. protocol BB84), after the transfer of all the states and the measurements Alice and Bob have two data strings. Using the open classical channel Alice and Bob announce their bases to each other, and they skip the fraction of data in which their bases did not coincide. Note that if the basis used for the sending of Alice, coincided with Bob's measurement basis, in the absence of noise in the communication channel results in their bit lines in the respective positions coincide, so after matching bases in the case of perfect channel and the lack of action by the interceptor Alice and Bob must have shared the same bit lines. However, if the channel introduced errors or interceptor tried to eavesdrop information in the bit strings of Alice and Bob, the data can be different, so they check the correlation by reveal in part of their bit strings. According to the central limit theorem, the error in the open bit sequences gives a fairly accurate estimate of errors in the entire sequence, and it is possible to accurately estimate the probability of error in the key. If the error value is above a certain threshold, data transfer is terminated: this means that the interceptor has too much information on the key. Otherwise, Alice and Bob can obtain the total secret key. This problem can be divided into two stages: the first is *correction of errors*, which result in the equivalent bit strings of Alice and Bob. The second phase, called *privacy amplification*, seeks to exclude key details that could get into the interceptor as a result of operations on quantum states or during error correction. As a result of this step in the interceptor should have no or minimum information on the common bit string of Alice and Bob.

Protocols on continuous variables are sensitive to environmental impact loss (noise) and thus require additional research. In addition, some protocols with continuous variables require random basis selection.

CHAPTER IV

Realistic channel in continuous-variable quantum key distribution

4.1 Effect of atmospheric channels on states

The protocols of quantum key distribution based on continuous variables (CV QKD), which are considered in the work are well studied and implemented in optical fiber transmission line. And when it comes to atmospheric optical communication line, then Gaussian channels require additional analysis. A feature of an atmospheric channel is that in free space attenuation is not fixed. The reason for this is that transparency changes due to atmospheric effects (turbulence). Such channel is characterized by fluctuating transmittance. However, the atmospheric links are important because they enable communication with no strict requirements to fiber infrastructure. And most importantly they allow the use of long-distance communication, such as satellite links. For protocols based on discrete variables, the effect of fluctuating channels is similar to the steady decay, which in turn reduces the transmission rate. However, in the case of continuous variables, the effect of fluctuating channel is more complex [18].

To investigate such fluctuating channels we consider the scheme of quantum communication as shown in the Figure 8:

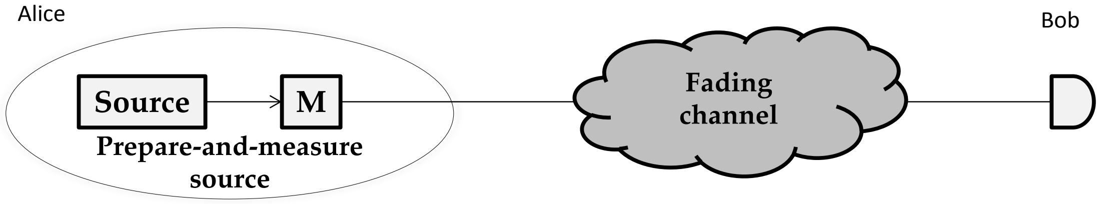

Figure 8

In such scheme Alice and Bob share an entangled two-mode squeezed vacuum state. Half of the entangled state is sent through a untrusted channel to Bob. Bob makes a homodyne measurement of the amplitude or phase quadrature. In its turn, when Alice measures both quadratures in a balanced heterodyne scenario, this is equivalent to *coherent state preparation* (Figure 9)

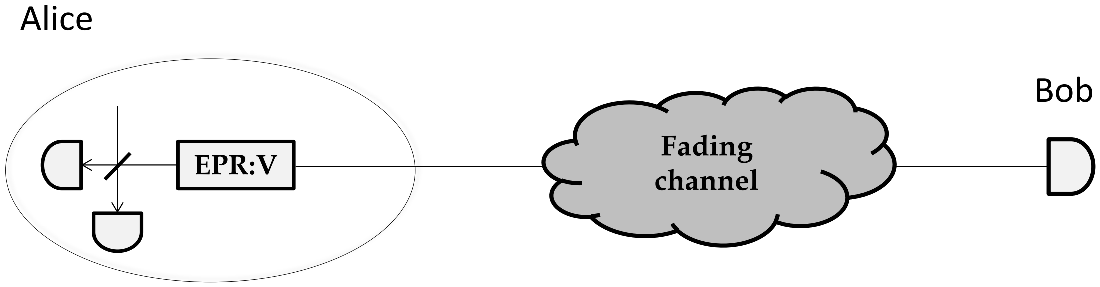

Figure 9

But when Alice measures single quadrature in a homodyne scenario, this is equivalent to *squeezed state preparation* (Figure 10):

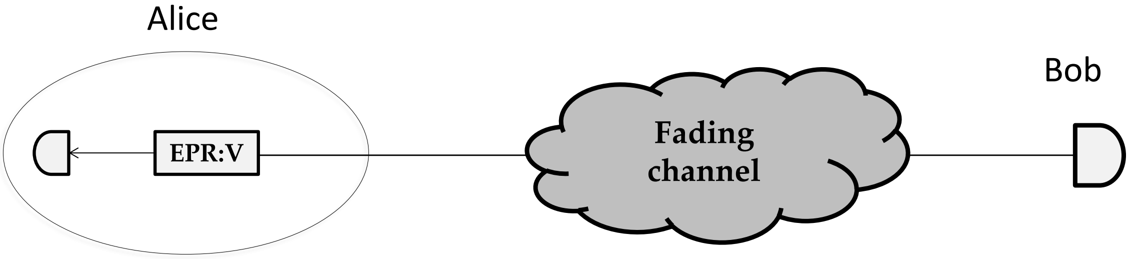

Figure 10

In our work the untrusted fading channel is atmospheric channel, therefore transmission varies due to turbulence. Such a channel (Figure11) can be described by a distribution of transmittance values $\{\eta_i\}$ with probabilities$\{p_i\}$.

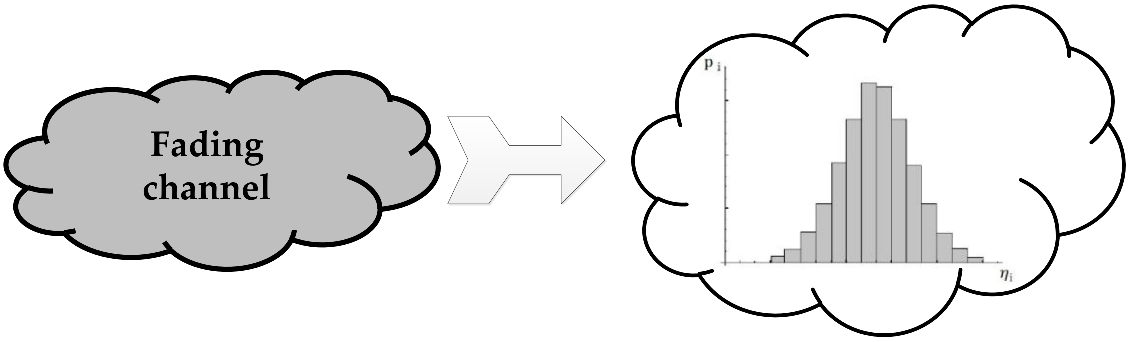

Figure 11

We deal with Gaussian states of light. Such states can be described by the covariance matrices as it was mentioned. The covariance matrix of two-mode squeezed vacuum state with variance $V \geq 1$, before the interaction has the form:

$$\gamma_{\mathrm{AB}} = \begin{pmatrix} V\mathbb{I} & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{I} \end{pmatrix} \quad (4.1)$$

where “$\mathbb{I}$” is the unity matrix

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (4.2)$$

and σ_z is the Pauli matrix

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (4.3)$$

After a channel with the mean value of transmittance $\langle\eta\rangle$ and the mean of square root of transmittance $\langle\sqrt{\eta}\rangle$ covariance matrix takes the form [19]:

$$\gamma'_{AB} = \begin{pmatrix} V\mathbb{I} & \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\sigma_z \\ \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\sigma_z & (V\langle\eta\rangle - \langle\eta\rangle + 1 + \epsilon_f + \chi)\mathbb{I} \end{pmatrix} \quad (4.5)$$

Here mode B:

$$V'_B = V\langle\eta\rangle - \langle\eta\rangle + 1 + \epsilon_f + \chi \quad (4.6)$$

contains excess noise caused by fading ϵ_f=Var ($\sqrt{\eta}$)(V-1), where Var($\sqrt{\eta}$) – the variance of channel transmittance, and χ – untrusted excess noise(detectors noise, untrusted channel noise) in the so-called “pessimistic scenario”. It was shown that fading channels may break the security of the coherent-state protocol [20]. In our work we consider entanglement-based protocol with homodyne detection.

4.2 Security analysis

For security analysis of the protocol the key rate was calculated in the case of individual and collective attacks. It is calculated as the difference between classical mutual information values, in the case of individual attacks, and as the difference between classical mutual information (between Alice and Bob) and Holevo quantity, which is calculated through von Neumann entropies, in the case of collective attacks, and will be shown later.

Individual attacks. As mentioned, we can effectively define fluctuating channel as a fixed channel, i.e. with constant transmittance also with present additional noise, which depends on the modulation. In this model the channel will contain untrusted noise, i.e. the noise in the channel. Therefore, for the calculation of individual attacks [21], we must apply the method of entangling Gaussian cloning machine, which was shown optimal [22]. In this case, Eve is represented by two modes of entangled state and carries out measurements on the second mode. The overall covariance matrix after such cloning attack (as on Figure 12) takes the form:

$$\begin{pmatrix} V\mathbb{I} & \sqrt{V^2-1}\sqrt{\eta}\sigma_z & -\sqrt{V^2-1}\sqrt{1-\eta}\sigma_z & 0 \\ \sqrt{V^2-1}\sqrt{\eta}\sigma_z & (\mathrm{V}\eta-\eta\mathrm{n}+\mathrm{n})\mathbb{I} & ((n-V)\sqrt{-(\eta-1)\eta})\mathbb{I} & \sqrt{n^2-1}\sqrt{1-\eta}\sigma_z \\ -\sqrt{V^2-1}\sqrt{1-\eta}\sigma_z & ((n-V)\sqrt{-(\eta-1)\eta})\mathbb{I} & (\mathrm{V}\eta-\eta\mathrm{n}+\mathrm{n})\mathbb{I} & \sqrt{n^2-1}\sqrt{\eta}\sigma_z \\ 0 & \sqrt{n^2-1}\sqrt{1-\eta}\sigma_z & \sqrt{n^2-1}\sqrt{\eta}\sigma_z & \mathrm{n}\mathbb{I} \end{pmatrix}$$

Figure 12

Here we can see two modes Alice and Bob, and two modes of Eve with initial variances *n*, to which Eve has to set cloner to make optimal attack. From covariance matrix after the interaction, we can write variance of the mode of Bob, which has the form:

$$\mathrm{V}'_{\mathrm{B}} = \mathrm{V}\eta - \eta\mathrm{n} + \mathrm{n} \qquad (4.6)$$

In this case, the initial variance of *n*, to which Eve has to set cloner to make optimal attack is

$$\mathrm{n} = (1 - \eta + \epsilon\mathrm{f} + \chi)/(1 - \eta) \qquad (4.7)$$

But given the fact that Eve measures the second mode as we should change the value n to $\frac{1}{n}$, when calculating the variance Bob at Eve.

Obtaining the necessary data from our quantum system we can calculate the key rate and the maximum channel fluctuation variance for protocol based on squeezed states.

Key rate is calculated as the difference of mutual information, the calculation of formulas which have been described above, and is written as follows:

for *direct reconciliation* (DR):

$$K_{DR} = I_{AB} - I_{AE} \tag{4.8}$$

for *reverse reconciliation* (RR):

$$K_{RR} = I_{AB} - I_{BE} \tag{4.9}$$

where I_{AB}, I_{BE}, I_{AE} is mutual information between the elements of communication. A positive the key rate indicates the security of the protocol.

In this case we are more interested in the reverse reconciliation, as that is more stable against loss, so we will consider only K_{RR}:

$$K_{RR} = \frac{\log(\frac{V(\eta(V-1)+(V-1)\mathrm{Var}+\chi+1)}{\eta+V(-\eta+(V-1)\mathrm{Var}+\chi+1)})}{\log(4)} - \frac{\log(\frac{(\eta(V-1)+(V-1)\mathrm{Var}+\chi+1)(\eta+V(-\eta+(V-1)\mathrm{Var}+\chi+1))}{V})}{\log(4)} \tag{4.10}$$

where “Var” is $\mathrm{Var}(\sqrt{\eta})$ – the variance of channel transmittance. Now we calculate the variance of channel transmittance, which breaks the security of the protocol.

$$Var(\sqrt{\eta})_{max,ind} = \frac{\eta}{V} - \frac{\chi}{V-1} \tag{4.11}$$

To evaluate the security of the protocol under the influence of channels we calculated the dependence of maximum variance regarding the level of modulation bandwidth (V). The same relationship is taken for protocol based on coherent states [20], to compare and assess the stability of the protocols to atmospheric effects, the maximum variance of the transmission of which is as follows:

$$Var(\sqrt{\eta})_{max,ind} = \frac{\eta\sigma+\sqrt{\eta^2\sigma^2+4(1+\sigma)^2}-2(1+\sigma)(1+\chi)}{2\sigma(1+\sigma)} \tag{4.12}$$

where σ:=V-1 corresponds to the variance of coherent state modulation in the prepare-and-measure scenario. And now we can make comparison between the protocols. In the Figure 13 can be seen maximal security - preserving Var($\sqrt{\eta}$) in the case of individual attacks for protocol based on squeezed state and for protocol based on coherent state versus the state variance V for different values of transmittance without untrusted excess noise $\chi = 0$ and with $\chi = 0.1$ untrusted excess noise (Figure 14).

Based on these comparisons, in the case of individual attacks, we can say that the quantum key distribution protocol based on squeezed states is more resistant to the effects of fluctuations than the protocol based on coherent states.

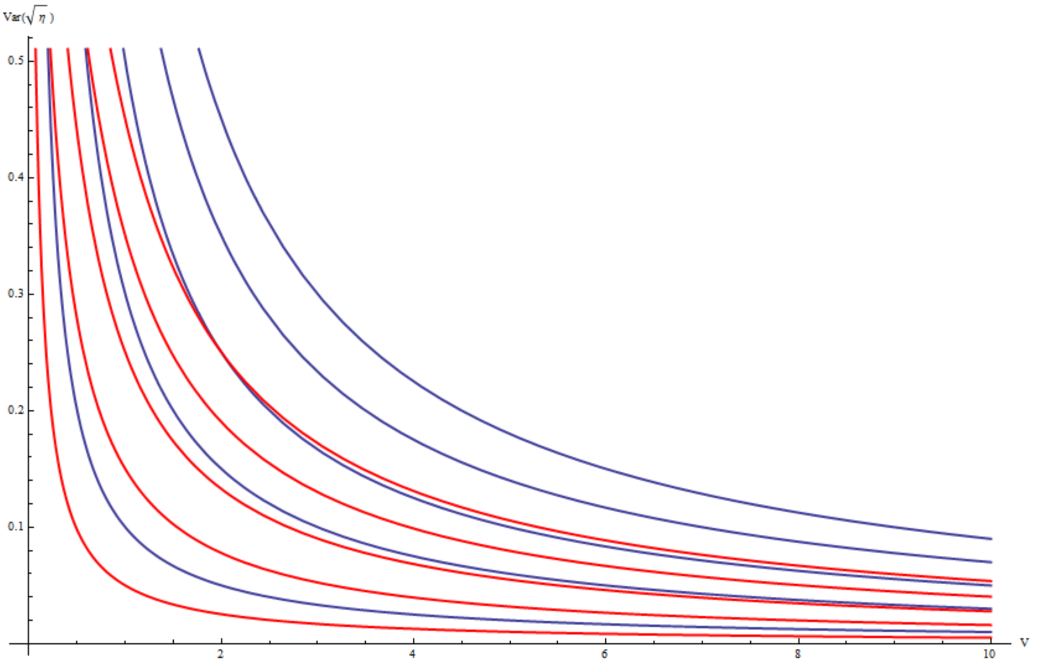

Figure 13 Maximal security-preserving Var($\sqrt{\eta}$) in the case of individual attacks for protocol based on squeezed state(solid blue lines) and for protocol based on coherent state(dashed red lines) versus the state variance V for different values of transmittance(from bottom to top: 0.1, 0.3, 0.5, 0.7, 0.9) without $\chi = 0$ untrusted excess noise.

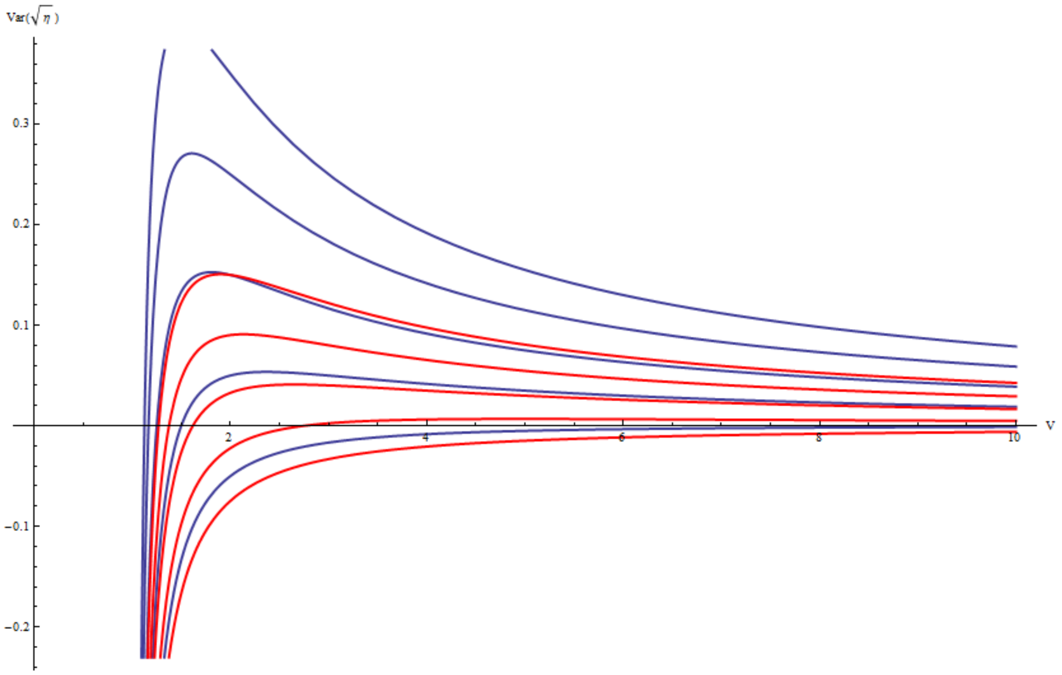

Figure 14 Maximal security-preserving Var($\sqrt{\eta}$) in the case of individual attacks for protocol based on squeezed state(solid blue lines) and for protocol based on coherent state(dashed red lines) versus the state variance V for different values of transmittance(from bottom to top: 0.1, 0.3, 0.5, 0.7, 0.9) with $\chi = 0.1$ untrusted excess noise.

And now we make comparison between the protocols in the more general case of collective attacks.

Collective attacks. In the case of collective attacks efficiency of the method of entangling Gaussian cloning machine is not proven. In this case, we will use covariance matrix after a channel with the mean value of transmittance $\langle\eta\rangle$ and the mean of square root of transmittance $\langle\sqrt{\eta}\rangle$, which was described in the previous section, and assume that Eve holds the purification of the state.

For security analysis of the protocol in the case of collective attacks the key rate was calculated as the difference between classical mutual information (between Alice and Bob) and Holevo quantity:

$$K_{RR} = I_{AB} - \chi_{BE} \tag{4.13}$$

where I_{AB} classical mutual information, which looks like:

$$I_{AB} = \frac{\log(\frac{V(\eta(V-1)+\chi+\epsilon\mathrm{f}+1)}{\eta+V(-\eta+\chi+\epsilon\mathrm{f}+1)})}{\log(4)} \tag{4.14}$$

and χ_{BE} Holevo quantity, which gives an upper bound for the leaked information, , which is calculated through von Neumann entropies

$$\chi_{BE} = G\left(\frac{\lambda_1-1}{2}\right) + G\left(\frac{\lambda_2-1}{2}\right) - G(\frac{\lambda_3-1}{2}) \tag{4.15}$$

where $G(x) = (x+1)\log(x+1) - xlogx$ is Bosonic entropic function, and λ_1, λ_2 are symplectic eigenvalues of the covariance matrix after a channel, and λ_3 which is calculated of conditional matrix

$$\gamma_A^B = \gamma_A - \sigma_{AB}(X\gamma_B X)^{MP}\sigma_{AB}^T \tag{4.16}$$

here we see $\gamma_A$and γ_B are the matrices, which describing the modes of Alice and Bob, and σ_{AB} is the matrix which characterizes correlations between the modes of Alice and Bob, and matrix X, which has the following form

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{4.17}$$

Now we can calculate the variance of channel transmittance, which breaks the security of the protocols. After that, we can make comparison between the protocol based on squeezed state and protocol based on coherent state (Figure 15, 16, 17) in the case without $\chi = 0$ untrusted excess noise and with $\chi = 0.012$ untrusted excess noises.

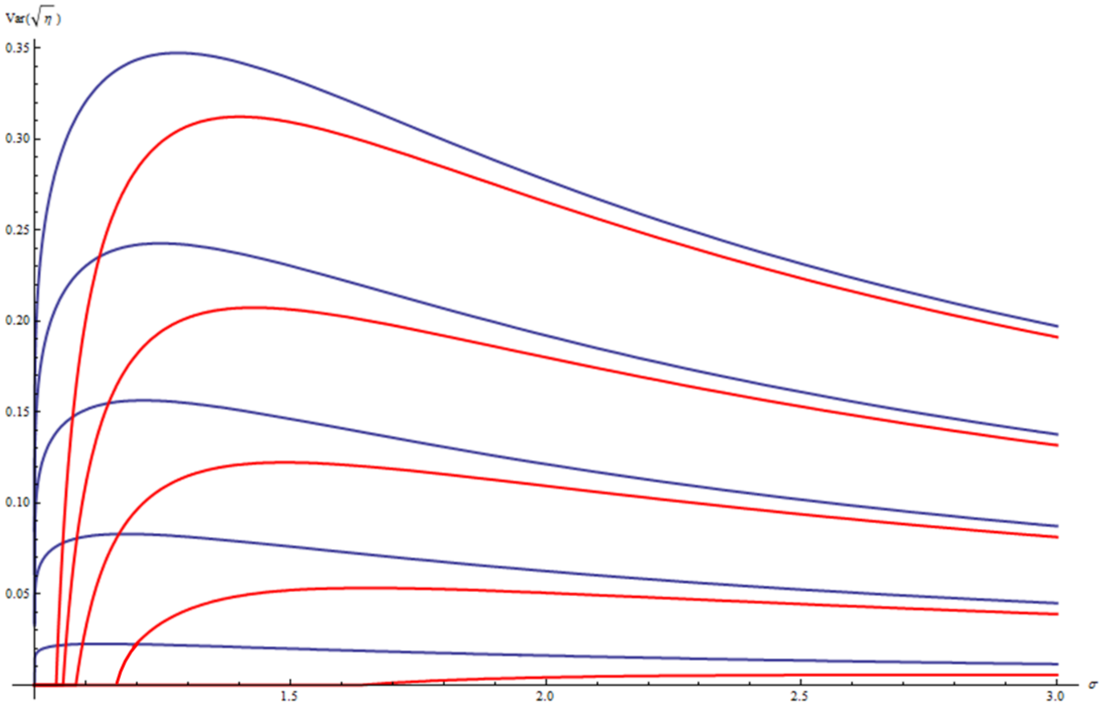

Figure 15 Maximal security-preserving Var($\sqrt{\eta}$) in the case of collective attacks for protocol based on squeezed state versus Gaussian modulation variance σ=V-1 for different values of transmittance (from bottom to top: 0.1, 0.3, 0.5, 0.7, 0.9) without($\chi = 0$) untrusted excess noise (solid blue lines) and with($\chi = 0.012$) untrusted excess noise (solid red lines).

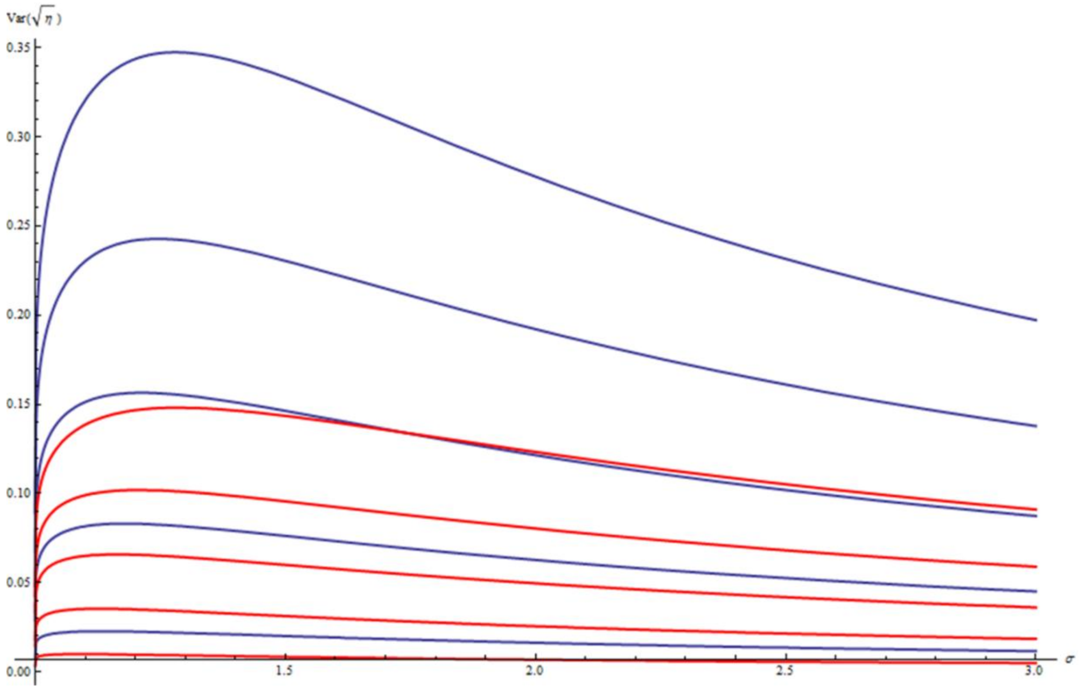

Figure 16 Maximal security-preserving Var($\sqrt{\eta}$) in the case of collective attacks for protocol based on squeezed state(solid blue lines)) and for protocol based on coherent state(solid red lines) versus Gaussian modulation variance σ=V-1 for different values of transmittance (from bottom to top: 0.1, 0.3, 0.5, 0.7, 0.9) without($\chi = 0$) untrusted excess noise

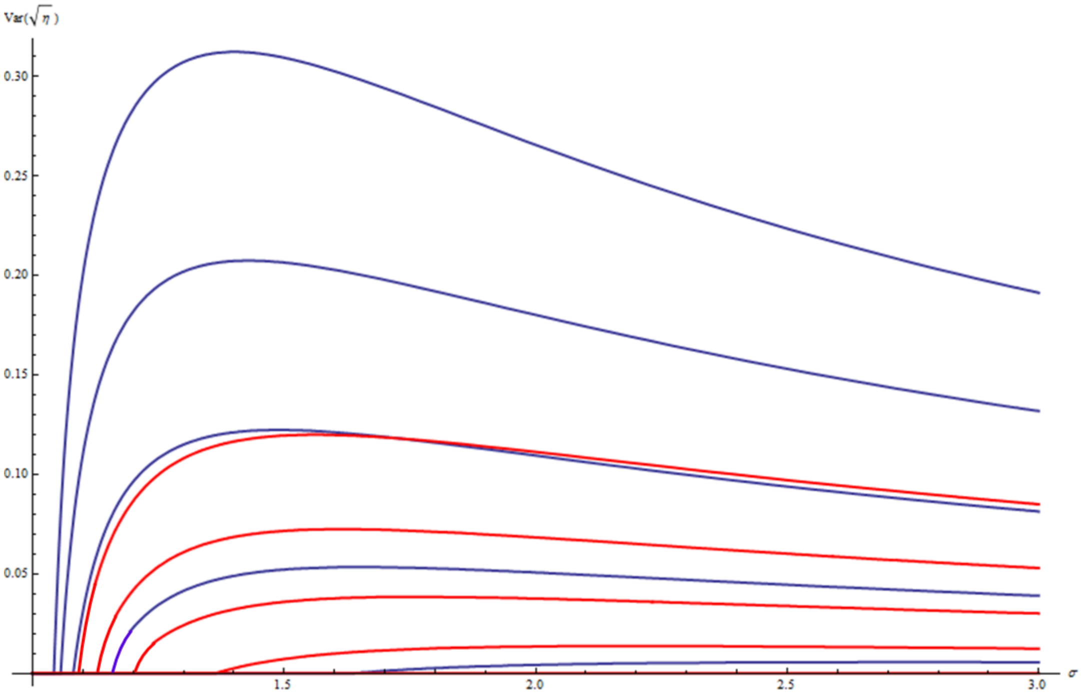

Figure 17 Maximal security-preserving Var($\sqrt{\eta}$) in the case of collective attacks for protocol based on squeezed state(solid blue lines)) and for protocol based on coherent state(solid red lines) versus Gaussian modulation variance σ=V-1 for different values of transmittance (from bottom to top: 0.1, 0.3, 0.5, 0.7, 0.9) with($\chi = 0.012$) untrusted excess noise

Evident from these comparisons is that the protocol based on squeezed state is more resistant to fluctuations than the protocol based on coherent states.

4.3 Location of the source

The next step of work is determining the optimal location of the source in the channel with fluctuations. We have two schemes with different source locations:

- source is located between two fading channels(Figure 18).

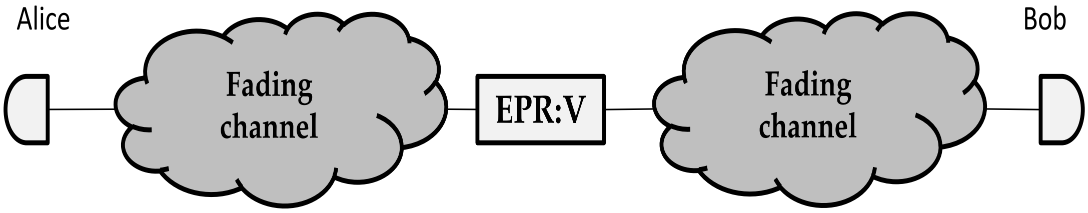

Figure 18

- sourcis located on the side of Alice(Figure 19)

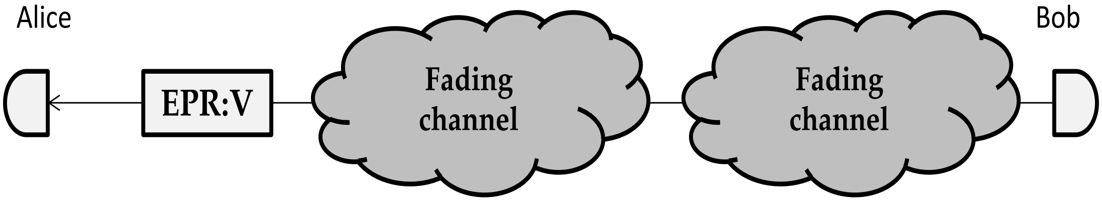

Figure 19

After a channel with the mean value of transmittance $\langle\eta\rangle$ and the mean of square root of transmittance $\langle\sqrt{\eta}\rangle$ corresponding covariance matrix cases will take the following form:

$$\gamma'_{AB} = \begin{pmatrix} (V\langle\eta\rangle - \langle\eta\rangle + 1)\mathrm{II} & \langle\sqrt{\eta}\rangle^2\sqrt{V^2-1}\sigma_z \\ \langle\sqrt{\eta}\rangle^2\sqrt{V^2-1}\sigma_z & (V\langle\eta\rangle - \langle\eta\rangle + 1)\mathrm{II} \end{pmatrix} \quad (4.18)$$

in case 1, and in case 2:

$$\gamma'_{AB} = \begin{pmatrix} V\mathbb{I} & \langle\sqrt{\eta}\rangle^2\sqrt{V^2-1}\sigma_z \\ \langle\sqrt{\eta}\rangle^2\sqrt{V^2-1}\sigma_z & (1-\langle\eta\rangle+\langle\eta\rangle(V\langle\eta\rangle-\langle\eta\rangle+1))\mathbb{I} \end{pmatrix} \qquad (4.34)$$

After calculations similar to those carried out in the previous section we can calculate the variance of channel transmittance, which breaks the security of the protocol. Finding it, we can make comparison of the two source locations, for the protocol based on squeezed state in the more general case of collective attacks(Figure 20).

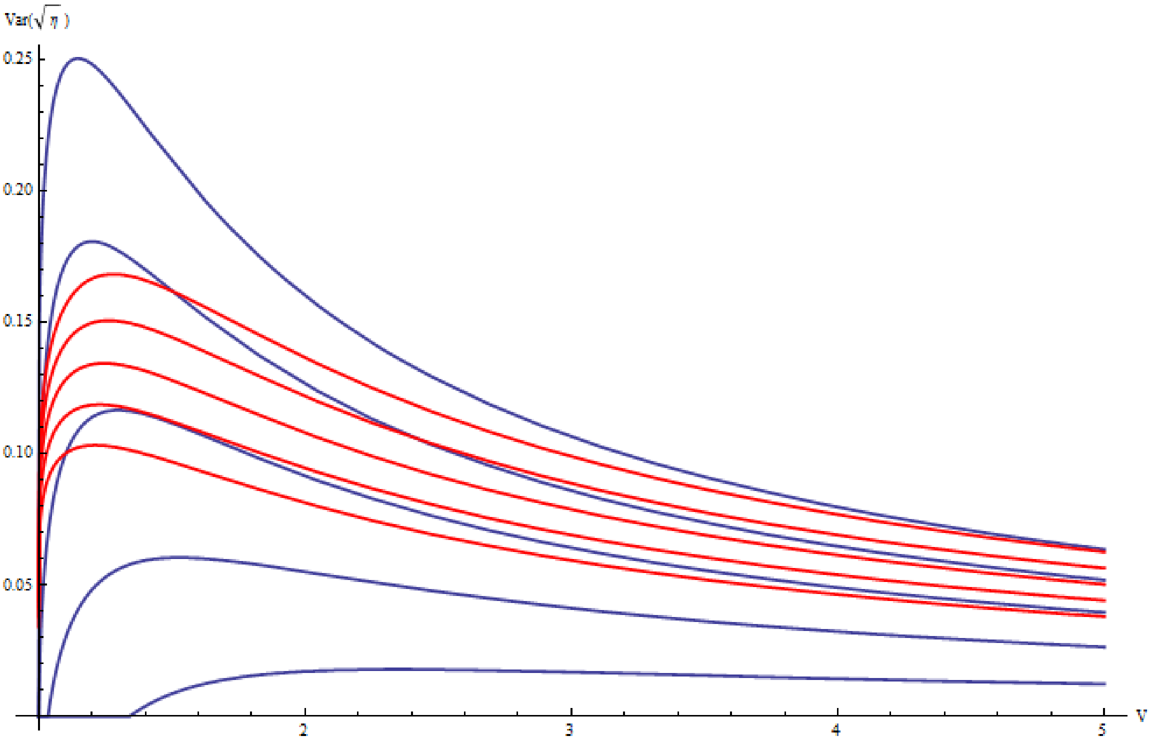

Figure 20 Maximal security preserving Var($\sqrt{\eta}$) for case 1 (solid blue lines) and for case 2 (solid red lines) versus state variance V for different values of $\langle\sqrt{\eta}\rangle^2$ (from bottom to top:0.5,0.6,0.7,0.8,0.9) without untrusted excess noise χ

From this result we can conclude that it is better to keep the source of entangled states on the side of Alice instead of placing it in the middle of a fluctuating channel.

CONCLUSIONS

In the thesis, using classical and quantum information theory we have estimated stability of the entangled-states based protocol against realistic atmospheric channel with fluctuations. We obtained the result in terms of the security-breaking fading variance and compared it to the result previously known for coherent-state protocol. It was shown, that protocol based on squeezed states is more resistant to realistic channel fluctuations than the coherent-state protocol. Also, we investigated and determined the optimal location of the source in the realistic fluctuating channel. It was shown, that the optimal position of the source is on the sender side of the channel.

ABBREVIATIONS

CV QKD	Continuous-variable quantum key distribution
RC4	Rivest Cipher 4
IDEA	International Data Encryption Algorithm
DES	Data Encryption Standard
AES	Advanced Encryption Standard
MAC	Message authentication codes
BB84	Quantum cryptography protocol by Charles Bennett and Gilles Brassard
PNS	Photon number splitting
EPR	Einstein, Podolsky and Rosen
DR	Direct reconciliation
RR	Reverse reconciliation

REFERENCES AND USED LITERATRE

[1] R. Feynman, Int. J. Theor. Phys. 21,467 (1982); D. Deutsch, Proc. R. Soc. London A 400, 97 (1985).

[2] P. Shor, *Proc. of 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society, Los Alamos, 1994), p. 124; S.I.A.M. Journal of Computing **26,** 1484 (1997);[quant-ph/9508027].

[3] Oded Goldreich, Foundations of Cryptography, Volume 1: Basic Tools, Cambridge University Press, 2001

[4] Bruce Schneier, Applied Cryptography, 2nd edition, Wiley, 1996

[5] Shannon, Claude (1949). "Communication Theory of Secrecy Systems". *Bell System Technical Journal* **28** (4): 656–715

[6] C. E. Shannon «A Mathematical Theory of Communication» (Translated in collections Shannon K. "work on the theory of information and cybernetics." - Moscow: IL, 1963. - 830 p., P 243-322)

[7] Shannon, Claude E. (July/October 1948). *Bell System Technical Journal* **27** (3): 379–423.

[8] Bennett *C.H.*, Brassard *G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc.of IEEE Int. Conf. on Comput. Svs, and Sign. Proees,, Bangalore, India, — 1984. — Pp. 175 -179

[9] D. Mayers and A. Yao, quant-ph/9802025.

[10] E. Biham, M. Boyer, P. O. Boykin, et al., quant-ph/9912053.

[11] P. W. Shor and J. Preskill, quant-ph/0003004. arXiv:quant-ph/0003004

[12] Einstein A., Podolsky B., Rosen N. *Phys. Rev. A - 1935. - Vol. 47, 777.* link.aps.org/doi/10.1103/PhysRev.47.777

[13] W. K. Wooters, W. H. Zurek, Nature 299, 802 (1982).

[14] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. 76, 2818 (1996)

[15] Raul GARCIA-PATRON SANCHEZ, «Quantum Information with Optical Continuous Variables:from Bell Tests to Key Distribution», Universite Libre de Bruxelles, Ph.D.Thesis(2007-2008)

[16] G. Brassard and L. Salvail "Secret key reconciliation by public discussion" Advances in Cryptology: Eurocrypt 93 Proc. pp 410-23 (1993)

[17] M. Hilleri, Phys. Rew. A.61,022309 (1999)

[18] Heersink J, Marquardt C, Dong R, Filip R, Lorenz S, Leuchs G and Andersen U L 2006 *Phys. Rev. Lett.* **96** 253601

[19] Dong R, Lassen M, Heersink J, Marquardt C, Filip R, Leuchs G and Andersen.U.L,2010 *Phys.Rev.* A 82 012312 CrossRef

[20] V. Usenko *et al* 2012 *New J. Phys.* **14** 093048

[21] Grosshans F and Grangier P 2002 Phys. Rev. Lett. 88 057902 CrossRef

[22] F. Grosshans, N.J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. 3, 535 (2003)