PALACKÝ UNIVERSITY OLOMOUC

Faculty of Science

Department of Optics

Side channels in continuous-variable quantum key distribution

Master thesis

Author:	Bc. Ivan Derkach
Study program:	N1701 Fyzika
Field of study:	Physics
Form of study:	Full-time
Supervisor:	Usenko Vladyslav, Dr.
Deadline:	26.04.2013

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

In Olomouc, ……. ……..

ACKNOWLEDGEMENT

It is with immense gratitude that I acknowledge the support and help of my supervisor Dr. Vladyslav Usenko. Without his guidance and persistent help this work would not have been possible.

I also consider it an honor to work with doc. Mgr. Radim Filip, Ph.D. and Mgr. Jaromír Fiurášek, Ph.D.

In addition I would like to thank my loved ones, who have supported me throughout entire process, both for constant encouragement and for helping me putting pieces together. I will be grateful forever for your love.

Bibliographical identification:

Author's first name and surname	Bc. Ivan Derkach
Title	Side channels in continuous-variable quantum key distribution.
Type of thesis	Master
Supervisor	Usenko Vladyslav, Dr.
The year of presentation	2013
Abstract	We address security of the quantum key distribution schemes based on squeezed and coherent state protocols with side channel and investigate how they are robust against excess noise and channel losses. While the presence of side channel does not destroy the security of protocols, it limits the robustness of both protocols to noise in the quantum channel. We consider method of compensating the negative influence of side channel by adding known modulated input noise. We show that an optimal value of noise that maximally compensate side channel influence for any quantum key distribution setup can be found.
Keywords	Quantum optics, quantum key distribution, continuous variables, Gaussian states,
Number of pages	55
Number of appendices	0
Language	English

Bibliografická identifikace:

Jméno a příjmení autora	Bc. Ivan Derkač
Název práce	Postranní kanály ve kvantové distribuci klíče se spojitými proměnnými.
Typ práce	Diplomová
Vedoucí práce	Usenko Vladyslav, Dr.
Rok obhajoby práce	2013
Abstrakt	V této práci byla studována bezpečnost protokolů kvantové distribuce klíče založených na stlačených a koherentních stavech s postranním kanálem a byla zemana jejich stabilita proti šumu a ztrát v kanálu. Přestože přítomnost postranného kanálu neničí bezpečnosti protokolů, ona omezuje stabilitu obou protokolů proti šumu ve kvantovém kanálu. Byl studován způsob kompenzace negativního vlivu postranného kanálu přidáním známého modulovaného vstupního šumu. Bylo ukázáno, že lze najít optimální hodnotu šumu, který maximálně kompenzuje vliv postranného kanálu pro dané nastavení protokolu.
Klíčová slova	Kvantová optika, kvantová distribuci klíče, spojité proměnné, gaussůvy stavy
Počet stran	55
Počet příloh	0
Jazyk	Anglický

Contents

1 Quantum Key Distribution protocols

1.1 Quantum key distribution.

Cryptography, the art of code-making and code-breaking, plays an important role in human history. Nowadays, as Internet and electronic business and transactions are an important part of modern world, cryptography has also became an essential part of our everyday life. With a well-developed cryptographic protocol, you can reasonably be sure that all your personal information is well protected whenever you make an online transaction. The evolution of cryptography has been propelled by endless war between code-makers and code-breakers, among whom are some of the brightest minds in human history. As soon as an existing code is broken, code-makers need to develop a stronger one to resume secure communication, which in turn stimulates code-breakers to attempt a new attack. The holy grail of cryptography is to develop an absolutely secure coding scheme which is secure against eavesdroppers with unlimited computational power. Surprisingly, this goal was achieved, at least in principle, when Gilbert Vernam invented the one-time pad (OTP) in 1917 [1].Like in many other modern cryptographic systems, a secure key is employed in the OTP encryption and decryption processes. While the encryption itself is publicly known, the security of the cryptographic system is guaranteed by the security of the key.

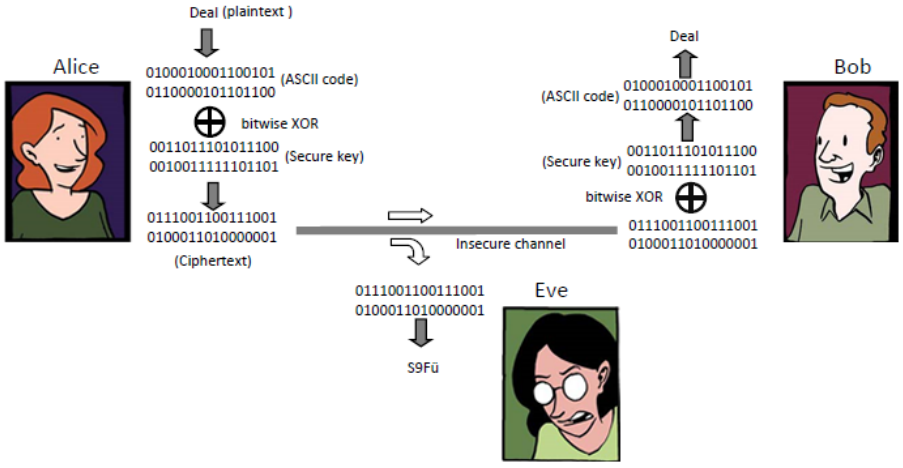

Figure 1: A cartoon illustrates one-time pad.Alice encodes her message, the ASCII code of - "deal", with a secure key by performing bitwise XOR operation. The cipher text is sent to Bob through an insecure communication channel. Bob can decipher the message by using the same secure key. Although Eve can also acquire a copy of the cipher text by wiretapping the comunication channel, without the secure key she cannot decode the original message.

As illustrated in 1.1, OTP is an encryption algorithm where the plain text

(a message understandable to anybody) is encoded with a secret random key (a pad) which has the same length as the plain text itself. The same key is also used by the legitimate receiver to decode the original message. Given that the random key is only used once, the absolute security of the OTP has been proved by Claude Shannon [2].

Although OTP is unbreakable in principle, there is a problem on applying this scheme in practice: once Alice and Bob have used up their pre-established secure key, the secure communication will be interrupted until they can acquire new key. This is the well-known key distribution problem which typically involves two unachievable tasks in classical physics: truly random number generation and unconditionally secure key distribution through an insecure channel. First of all, the deterministic nature of classical physics, which is implied by Albert Einstein's famous quotation — "God doesn't play dice", rules out the existence of truly random numbers in chaotic, but classical, processes. In contrast, truly random numbers can be generated from elementary quantum processes[3]. Secondly, in a world where information is encoded classically, there is no secure scheme to distribute a key through an insecure channel (otherwise, Alice and Bob could employ the same scheme to send secure messages directly). The fundamental reason is that in classical physics, information can be duplicated. Alice and Bob cannot prove that a key established through an insecure channel has not been copied by Eve. The only conceivable but cumbersome way to perform key distribution is by sending trusted couriers. Due to this key distribution problem, OTP has been adopted only when extremely high security is required.

In most of modern cryptographic systems such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES), much shorter keys are used to encrypt long messages. This reduces the consumption of random keys but does not fully solve the key distribution problem. Furthermore, these protocols are not as secure as the OTP.

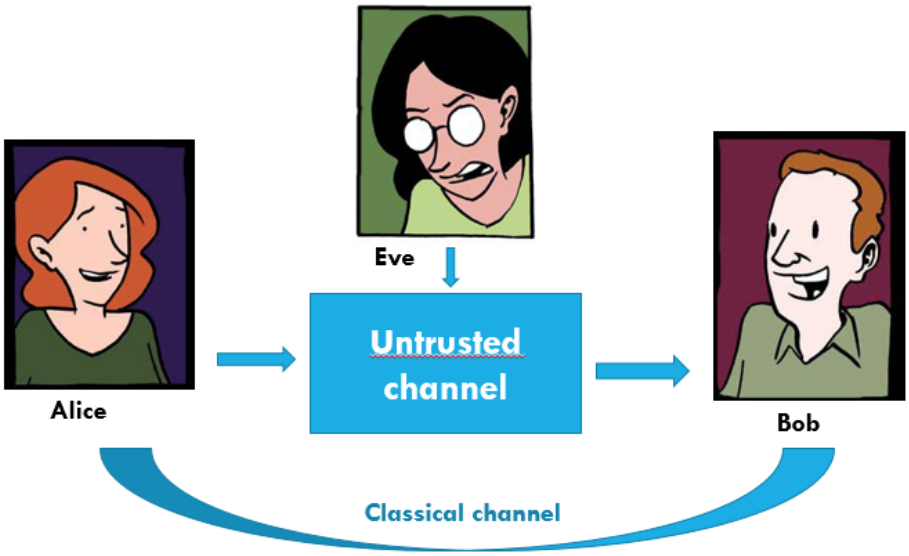

Figure 2: General key distribution scheme

To fully solve the key distribution problem, public key cryptographic protocols, including the famous RSA scheme (named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman), have been invented[4]. RSA is an asymmetric key algorithm where the message receiver, Bob, prepares two different cryptographic keys—a public key and a private key. Bob broadcasts the public key through an authenticated channel so that everyone who listens to this channel can acquire a copy of the public key. The message sender, Alice, encodes her message with the public key from Bob and sends out the encrypted message through a public insecure channel. This algorithm has been designed in such a way that a message encrypted with a public key can only be decrypted with the corresponding private key.

Public key cryptographic algorithms overcome the key distribution problem and have been widely adopted in today‘s cryptographic systems. Unfortunately, their security rests upon unproven mathematical assumptions. For example, the security of RSA is based on the assumption that there is no efficient way to find the prime factors of a large integer. However, this assumption has not been proved despite the tremendous efforts from mathematicians. Given the fact that RSA itself was an unexpected discovery, we cannot rule out the possibility that someone could find an efficient factoring algorithm and thus compromise most public cryptographic systems. Moreover, an efficient factoring algorithm running on a quantum computer exists [5]. This suggests that as soon as the first large-scale quantum computer switches on, most of today‘s cryptographic systems could collapse overnight.

It is true that the realization of a large-scale quantum computer could be still decades away. However, its potential threat to today‘s information security

cannot be neglected. We can imagine that a powerful Eve could record today's communications and decode the information when a quantum computer is available. This is a realistic problem since some information, such as military communications and health records, need to be secure for a long term.

It is interesting to notice that one decade before people realized that a quantum computer could be used to break public key cryptography, they had already found a solution against this quantum attack—quantum key distribution (QKD)[6]. Based on the fundamental principles of quantum physics, QKD provides an unconditionally secure way to distribute random keys through insecure channels. The secure key generated by QKD could be further applied in the OTP scheme or other encryption algorithms to enhance information security.

There are lots of protocols for QKD based on various types of quantum states that carry the encoded information, types of reconciliation, light sources and etc. but the main participants of key distribution, as in case of classical information distribution, stay the same – Alice "the sender", Bob "the receiver" and malicious and powerful Eve "the eavesdropper". First of all we make an assumption that Eve possess unlimited computational capabilities and is limited only by laws of physics. Secondly Alice and Bob share 2 channels, one fully classical and other one where quantum carriers of information propagate.

Quantum key distribution begins with the transmission of single or entangled quanta between Alice and Bob. Eavesdropping, from physical point of view, is based on a set of measurements performed by an eavesdropper on carries of information, in this case on the transmitted quanta. According to the rules of quantum mechanics, in general, any measurement performed by Eve unavoidably modifies the state of the transmitted quanta and this can be discovered by Alice and Bob in a subsequent public communication. Thus the main ingredients of QKD systems are: a quantum "untrusted" channel for the exchange of quanta and the so-called public channel, which is used to test whether or not the transmission through quantum channel is distorted. Any public channel can be freely monitored by anybody, however it should be impossible to modify the information sent through such a channel.

All QKD protocols have one general scheme. In it Alice on her side prepares the state, encodes information into it and then sends it to Bob through untrusted quantum channel, by "untrusted" we understand a channel (air, optical fiber) that is under Eve's control. After Bob detected the state, he and Alice use classical channel for information reconciliation. Both of them do not send information about detection results through classical channel, so even if Eve is eavesdropping it, it would not increase her information about the key. So why is this more secure than modern cryptographic systems?

1.2 The principles of quantum cryptography

1.2.1 No-cloning theorem

In 1982, N. Herbert proposed a superluminal communication scheme by employing Einstein–Podolsky–Rosen (EPR) pair and by allowing perfectly cloning

of an unknown quantum state [7]. This proposal directly conflicts with special relativity and aroused active discussions in the scientific community. Shortly afterwards, W.K.Wootters and W.H. Zurek [8] and D. Dieks [9] independently discovered quantum no-cloning theorem, thus disproving Herbert's superluminal communication scheme.

Quantum no-cloning theorem states that an arbitrary quantum state cannot be duplicated perfectly. This theorem is a direct result of the linearity of quantum physics. Quantum no-cloning theorem is closely related to another important theorem in quantum mechanics, which states: if a measurement allows one to gain information about the state of a quantum system, then in general the state of this quantum system will be disturbed, unless we know in advance that the possible states of the original quantum system are orthogonal to each other [8].

Instead of providing a mathematical proof of quantum no-cloning theorem, we simply discuss two examples to show how it works. In the first case, we are given a photon whose polarization is either vertical or horizontal. To determine its polarization state, we can send it through a polarization beam splitter followed by two single photon detectors. If the detector at the reflection path clicks, we know the input photon is vertically polarized, otherwise it is horizontally polarized. Once we know the polarization state of the input photon, we can prepare arbitrary number of photons in the same polarization state. Equivalently, we have achieved perfect cloning of the polarization state of the photon. This is because the two possible polarization states of the input photon are orthogonal to each other. In the second case, we are given a photon whose polarization is randomly chosen from a set of {horizontal, vertical, 45°, 135°}. Since the four polarization states given above are linearly dependent, it is impossible to determine its polarization state from any experiment. For example, if we use the same polarization beam splitter mentioned above, a 45° polarized photon will have a $50/50$ chance to be either reflected or transmitted, therefore it cannot be determined with certainty.

One common question is why an optical amplifier, which has been widely used in optical communication to boost optical power, cannot be used to copy photons. Actually, in the original superluminal communication scheme, Herbert did mistakenly assume that the receiver could make perfect copies of the input photon with an optical amplifier[7]. As pointed out by Wootters, the impossibility of making perfect copies of photon through stimulated emission process originates from the unavoidable spontaneous emission: while the stimulated photon is a perfect copy of the incoming one, the spontaneous emitted photon has a random polarization state[**?**].

At first sight, the impossibility of making perfect copies of unknown quantum states seems to be a shortcoming. Surprisingly, it can also be an advantage. It turned out that by using this impossibility smartly, unconditionally secure key distribution could be achieved: any attempts by the eavesdropper to learn the information encoded quantum mechanically will disturb the quantum state and expose her existence.

Quantum key distribution protocols can be divided into 2 branches: discrete

variable and continuous-variable protocols. For better understanding of main principles and mechanics of QC it is convenient to start with the first proposed discrete-variable protocol.

1.2.2 The BB84 protocol

Proposed in 1984 by Charles H. Bennet and Gilles Brassard it was the the first quantum cryptography protocol [6]. The protocol is based on 2-level information carrier systems (qubits). Information can be encoded in photon polarization states, electron spins etc. We will use photon polarization as a most common example. Alice transmits photons to Bob in one of four different polarization states: horizontal (H), vertical (V), diagonal (D, $45\,^\circ$) and anti-diagonal (A, $-45\,^\circ$). For each photon she sends, Alice randomly selects one of these polarizations, with H or D representing the bit value "0" and V or A representing "1", depending on the "basis" she chooses. To measure the photons, Bob is equipped with an analyzer that can distinguish either between H and V ($+$) or between A and D ($\times$). He randomly (and independently from Alice) chooses which analyzer he will use to measure each photon. If Bob selects the analyzer that is compatible with Alice's choice, he will determine the photon's polarization, and thus the bit value, with certainty. If, on the other hand, Bob measures with the "wrong" analyzer, he will obtain a random result.

It seems problematic that half of Bob's measurements result in a random bit value. However, Alice and Bob have a cunning solution. After Bob's measurements have taken place, he reveals the sequence of analyzers that he used. Alice then tells him which times he used the correct analyzer, without revealing the bit that she sent. They can then discard all the measurements for which Bob used the wrong analyzer, ensuring that they share the same bit sequence without any errors (in the absence of noise or imperfections).

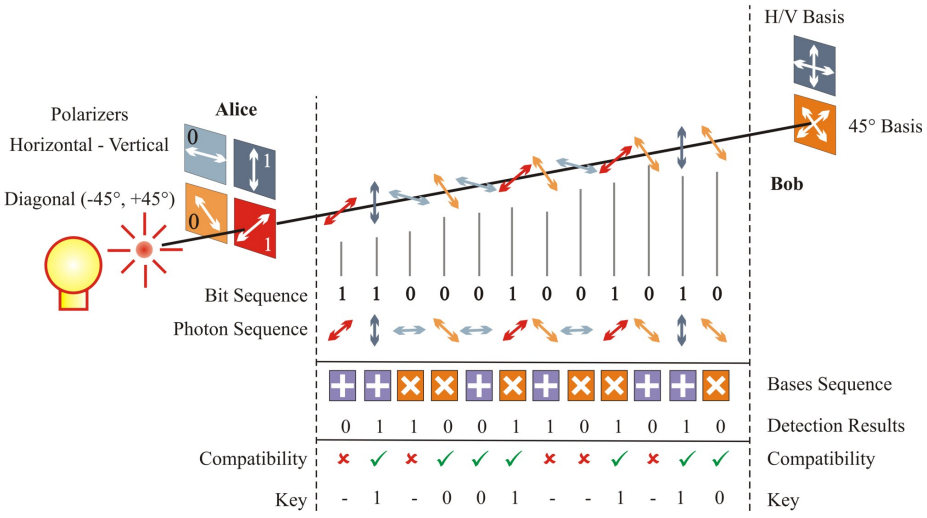

Figure 3: BB84 protocol. Alice encodes bit sequence onto photon polarization states and sends them to Bob, who chooses measurement bases, detects photons an obtains another bit sequence. Alice and Bob use classical channel to check whether Bob used a proper basis for every individual measurement therefore they "sift" second bit sequence and obtain secure key.

This post-selection leaves an eavesdropper (Eve) at a disadvantage since she must guess which analyzer to use to measure each photon (bottom). Inevitably Eve will sometimes select an analyzer that is incompatible with Alice's choice of polarization, and thus may obtain a result that differs from the bit Alice sent. The key to the secrecy of quantum cryptography is that by making this measurement, Eve inevitably changes the quantum state of the photon. Therefore, when Bob receives the photon, he will sometimes determine an erroneous bit value even when he and Alice used compatible measurements. By examining a small sample of their bit sequence for errors, Alice and Bob can therefore determine whether an eavesdropper was present.

At this point in the BB84 protocol, Alice and Bob share a so-called sifted key. But this key contains errors. The errors are caused by technical imperfections, as well as possibly by Eve's intervention. Realistic error rates in the sifted key using today's technology are of the order of a few percent. The last step of any quantum cryptography protocol is to use classical algorithms to correct the errors and then to reduce Eve's information on the final key. The latter process is called *privacy amplification*. With the simplest error correction protocol, Alice randomly chooses pairs of bits and announces their XOR value. Bob replies either "accept" if he has the same XOR value for his corresponding bits, or "reject" if not. In the first case, Alice and Bob keep the first bit of the pair and discard the second one, while in the second case they discard both bits. In reality, more complex and efficient algorithms are used. After error

correction, Alice and Bob have identical copies of a key, but Eve may still have some information about it. Alice and Bob thus need to reduce Eve's information to an arbitrarily low value using some privacy amplification protocols. These classical protocols typically work as follows. Alice again randomly chooses pairs of bits and computes their XOR value. But, in contrast to error correction, she does not announce this XOR value. She only announces which bits she chose (e.g., bits number 103 and 537). Alice and Bob then replace the two bits by their XOR value. In this way they shorten their key while keeping it error free, but if Eve has only partial information on the two bits, her information on the XOR value is even less. Assume, for example, that Eve knows only the value of the first bit and nothing about the second one. Then she has no information at all about the XOR value. Also, if Eve knows the value of both bits with 60% probability, then the probability that she correctly guesses the XOR value is only $0.6^2 + 0.4^2 = 52\%$. This process would have to be repeated several times; more efficient algorithms use larger blocks [10].

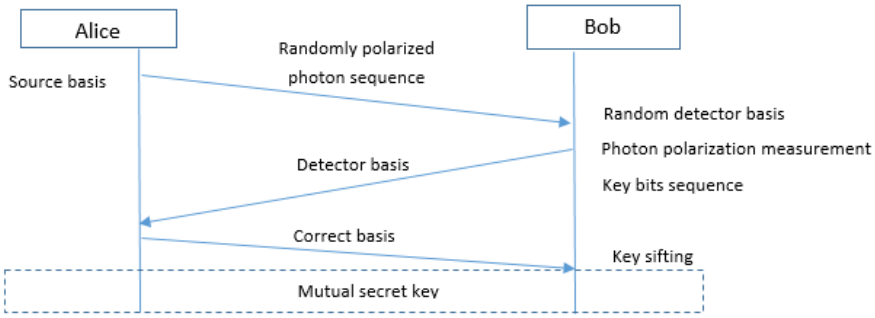

Figure 4: Information exchange between sender and receiver

1.2.3 Entanglement based QKD

Since Einstein, Podolsky and Rosen published their well-known paper in 1935[11], entanglement phenomena has become one of the most puzzling and yet attractive feature in quantum mechanics. Quantum entanglement occurs when pair of particles such as photons, electrons and even molecules is properly described by the same quantum mechanical description (state), which is indefinite in terms of important factors such as position, momentum, spin, polarization, etc. From a phenomenological point of view, the phenomenon of entanglement is fairly simple. When two physical systems come to an interaction, some correlation of a quantum nature is generated between the two of them, which persists even when the interaction is switched off and the two systems are spatially separated[1]. If

[1] Entanglement can be also created without direct interaction between the subsystems, via the so-called entanglement swapping[12]

we measure a local observable on the first system, its state collapses of course in an eigenstate of that observable. Surprisingly, also the state of the second system, wherever it is (in the ideal case of zero environmental decoherence), is modified instantly. Responsible for this "spooky action at a distance" is the non-classical and non-local quantum correlation known as entanglement. To illustrate how entanglement can be used in QKD, let us discuss some properties of a polarization-entangled photon pair.

An arbitrary polarization state of a single photon can be described as a superposition of two basis states:

$$|\psi\rangle_{singlephoton} = \alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle$$

where $|\updownarrow\rangle$and $|\leftrightarrow\rangle$represent vertical and horizontal polarization states, forming a set of orthogonal bases, $\alpha$and β are complex numbers that should satisfy the normalization condition $\alpha\alpha^* + \beta\beta^* = 1$. In this simple example we assume that the state we describe is pure and there is a well-defined phase relation between the two basis components. The most general pure polarization state of a photon pair can be described by a superposition of four basis states:

$$|\psi\rangle_{photonpair} = \alpha_1\,|\updownarrow\rangle_1\,|\updownarrow\rangle_2 + \alpha_2\,|\updownarrow\rangle_1\,|\leftrightarrow\rangle_2 + \alpha_3\,|\leftrightarrow\rangle_1\,|\updownarrow\rangle_2 + \alpha_4\,|\leftrightarrow\rangle_1\,|\leftrightarrow\rangle_2$$

where $|\updownarrow\rangle_1\,|\updownarrow\rangle_2$ is a basis state state in which both photons are in vertical polarization state, other terms in the equation are understood in a similar way.

In special case when$\alpha_1 = \alpha_4 = \frac{1}{\sqrt{2}}$ and $\alpha_2 = \alpha_3 = 0$, entangled photon pair state can be written as

$$|\Phi\rangle_{pair} = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle_1\,|\updownarrow\rangle_2 + |\leftrightarrow\rangle_1\,|\leftrightarrow\rangle_2\right)$$

One special feature of the above state is that it cannot be described by a tensor product: $|\Phi\rangle_{pair} \neq |\psi\rangle_1 \otimes |\psi\rangle_2$, where $|\psi\rangle_1$ and $|\psi\rangle_2$ are arbitrary single photon polarization states. In other words, the two photons are "entangled" with each other. Entangled photons can present no-local correlation which doesn't exist in classical physics.

Now suppose we send one photon of an EPR pair to Alice and the other one to Bob. If Alice measures her photon in the rectilinear basis, she will detect a vertical or a horizontal polarized photon with the same probability. Depending on Alice's measurement result, Bob's photon will be projected to the corresponding polarization state. If Bob subsequently measures his photon in the same basis, his measurement result will be perfectly correlated to Alice's result. On the other hand if Bob measures in diagonal basis, no correlation exists. The situation will stay the same if Bob will perform measurement first. Alice and Bob will get perfect correlation also in case when both of them measure in diagonal basis:

$$|\Phi\rangle_{pair} = \frac{1}{\sqrt{2}}\left(|\nearrow\rangle_1\,|\nearrow\rangle_2 + |\nwarrow\rangle_1\,|\nwarrow\rangle_2\right)$$

where $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle + |\leftrightarrow\rangle)$represents 45° polarization state and $|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle - |\leftrightarrow\rangle)$represents 135° polarization state.

The discussion above suggests that Alice and Bob can implement BB84 type QKD based on an EPR source. The EPR source can be placed between Alice and Bob. One photon of each EPR pair is sent to Alice and the other one to Bob. For each incoming photon, Alice and Bob randomly and independently choose their measurement bases to be either rectilinear or diagonal. After the transmission has taken place, Alice and Bob can announce in public the orientations of the analyzers they have chosen for each particular measurement.

An eavesdropper, Eve cannot elicit any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there. The information "comes into being" only after the legitimate users perform measurements and communicate in public afterwards. Eve may try to substitute her own prepared data for Alice and Bob to misguide them, but as she does not know which orientations of the analyzers will be chosen for a given pair of particles there is no good strategy to escape being detected. In this case her intervention will be equivalent to introducing elements of physical reality to the polarization directions.

The above QKD protocol based on EPR pairs is quite similar to the original BB84 QKD. However, there is much more physical insight in the first entanglement based QKD protocol proposed by Ekert in 1991[13], especially the deep connection between entanglement and the security of QKD. In his original proposal, Ekert suggested that Alice and Bob can verify entanglement by testing a certain type of Bells inequalities[1]. As long as they can verify the existence of entanglement, it is possible to generate secure key.

1.2.4 Continuous-variable protocols

Previously mentioned protocol and its configurations are called discrete-variable protocol, because the carrier of information in them is a single qubit, speaking in other words, 1 bit of information is encoded into 1 photon. These types of protocols have one disadvantage: one-photon signal that is sended to the receiver can be correctly detected only with a small probability, besides it can also be completely lost in the channel. So occurred a problem of creation of protocols that would have all (or at least most of them) measurements more informative. This can be achieved by encoding information into multi-photon states, continuous variables.

The first continuous-variable protocol was developed by Hillery[14]. In 2000 he suggested a scheme, which is based on using a squeezed light. The states of light are squeezed in one of two field quadrature components, and the value of the squeezed component is used to encode a character from an alphabet. The uncertainty relation between quadrature components prevents an eavesdropper from determining both with enough precision to determine the character being sent. Suggested scheme requires a high squeezing that can be pretty challenging from technical point of view. Losses degrade the performance of this scheme, but it is possible to use phase sensitive amplifiers to boost the signal and partially

compensate for their effect. One should notice and stress out that unlike the information encoded into polarization state of the single photon this scheme encodes information into quadratures and can have a much bigger alphabet for photons than "1" and "0".

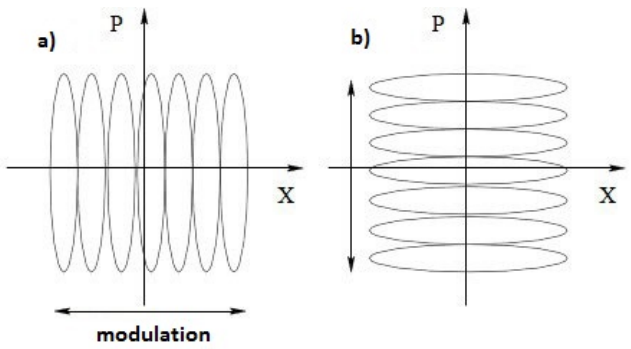

Figure 5: Squeezed state modulation in phase space, a) x- quadrature and b) p-quadrature

Later in 2001, protocol was improved by Cerf [15]. He suggested to use Gaussian distribution modulation instead of just random modulation. Basically he suggested to apply Gaussian noise, stressing out that this makes continuous not only variable but key itself, and it is later discretized with the help of additional security enhancing algorithms.

Whereas realization of protocols with squeezed light is relatively complicated, coherent states were suggested as carriers of encoded information by Grosshans and Grangier in 2002[16]. Using coherent states also allows to encode information in both quadratures. In other suggested by Silberhorn [16] protocol similarly to E91, Alice does not prepares a state but uses an EPR source and key is generated randomly during measurement processes.

- Efficiency of homodyne or heterodyne detections ($\backsim$90%) that are being used in continuous-variable protocols is much higher than of single-photon detectors ($\backsim$30%) that are necessary in discrete variable protocols.
- Homodyne detectors can process information much faster than single-photon detectors.
- Gaussian states for continuous variable protocols are easier to generate comparing to single photons that are needed for discrete variable protocols.

Unlike single-photon protocols, where qubits either arrive to Bob's side or can be renewed after compensation of environmental influence, continuous-variable protocols are very sensitive to continuous influence of environment that cannot be compensated. Influences of losses and noise should always be taken into account for these types of protocols.

2 Basics of continuous-variable protocols

2.1 Introduction to continuous-variable systems

A continuous-variable system of N canonical bosonic modes is described in a Hilbert space

$$\mathscr{H} = \bigotimes_{k=1}^{N} \mathscr{H}_k \tag{1}$$

resulting from the tensor product structure of infinite-dimensional Fock spaces $\mathscr{H}_k$'s. Modes of the quantized electromagnetic field can have different energies, polarizations etc. The space $\mathscr{H}_k$ is spanned by the Fock basis $\{|n\rangle_i\}$ of eigenstates of the number operator $\hat{n_k} = \hat{a}_k^\dagger \hat{a}_k$. The vacuum state of the global Hilber space can written as $|0\rangle = \otimes_k |0\rangle_k$, where $\hat{a}_k |0\rangle_k = 0$ is the ground state of the Hamiltonian that describes a system of N harmonic oscillators (modes of the quantized electromagnetic field),

$$\hat{\mathcal{H}} = \sum_{k=1}^{N} \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right) \tag{2}$$

here $\hat{a}_k^\dagger$ and $\hat{a}_k$ are the creation and annihilation operators of a photon in mode k (with frequency ω_k) which satisfy the bosonic commutation relation,

$$\left[\hat{a}_k, \hat{a}_l^\dagger \right] = \delta_{kl}, \ [\hat{a}_k, \hat{a}_l] = \left[\hat{a}_k^\dagger, \hat{a}_l^\dagger \right] = 0 \tag{3}$$

The corresponding quadrature phase operators (analogy to classical position and momentum) for each mode are defined as

$$\hat{x} = \hat{a}^\dagger + \hat{a} \tag{4}$$

$$\hat{p} = i \left(\hat{a}^\dagger - \hat{a} \right) \tag{5}$$

Quadrature operators can be grouped in the vector

$$\hat{r} = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \ldots, \hat{x}_N, \hat{p}_N)^T \tag{6}$$

which enables us to write in a compact form the bosonic commutation relations between the quadrature operators,

$$[\hat{r}_i, \hat{r}_j] = i\Omega_{ij} \tag{7}$$

where Ω is the symplectic form

$$\Omega = \bigoplus_{i=1}^{N} \omega, \ \ \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{8}$$

In single-mode Hilbert space $\mathscr{H}_k$, the eigenstates of $\hat{a}_k$constitute the important set of coherent states. Coherent states result from applying the single-mode Weyl displacement operator $\hat{D}_k$ to the vacuum $|0\rangle_k$, $|\alpha\rangle_k = \hat{D}_k(\alpha) |0\rangle_k$, where

$$\hat{D}_k(\alpha) = \mathrm{e}^{\alpha\hat{a}_k^\dagger - \alpha^* \hat{a}_k} \tag{9}$$

and the coherent amplitude $\alpha \in \mathbb{C}$ satisfies $\hat{a}_k |\alpha\rangle_k = \alpha |\alpha\rangle$. Weyl operator is the generalization to N modes of the displacement operator.

2.2 Quantum phase-space picture

The states of a CV system are the set of positive density operators (ρ) on the Hilber space $\mathscr{H}$. However, the complete description of any quantum state can be provided by the characteristic function which is the Fourier transform of the quasi-probability distribution, the so called Wigner function. This also allows us to refer quantum states to functions defined on the phase-space. In terms of Weyl operator Wigner function can be written as

$$\chi_\rho(\xi) = \mathrm{Tr}\left[\rho D_\xi\right] \tag{10}$$

with vector ξ that belongs to the real 2N-dimensional space$\left(\xi \in \mathbb{R}^{2\mathrm{N}}\right)$, which is called phase-space. Every characteristic function responds to a certain state, and they are related with each other via a Fourier-Weyl relation. An arbitrary state ρ can be written from its characteristic function:

$$\rho = \frac{1}{(2\pi)^N} \int d^{2N}\xi \chi_\rho(-\xi) D_\xi \tag{11}$$

The Wigner function being the quasi-probability distribution is used for another set of complete description of the quantum states

$$W(\xi) = \frac{1}{(2\pi)^N} \int d^{2N}\varsigma \mathrm{e}^{i\xi^T \Omega \varsigma} \chi_\rho(\varsigma) \tag{12}$$

For a Gaussian state, its Wigner function is also a Gaussian function. After performing the Gaussian integration, we obtain

$$W(\xi) = \frac{1}{\pi^{2N}\sqrt{\det\gamma}} \mathrm{e}^{-(\xi - D)^T \gamma^{-1} (\xi - D)} \tag{13}$$

here, $\gamma > 0$ is a symmetric matrix. In the picture of distribution function, an n-mode Gaussian state is characterized by the $2n$-dimensional covariance matrix γ and the $2n$-dimensional displacement vector D.

$$\gamma = \begin{pmatrix} \gamma_1 & \sigma_{1,2} & \cdots & \sigma_{1,n} \\ \sigma_{1,2}^T & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \sigma_{n-1,n} \\ \sigma_{1,n}^T & \cdots & \sigma_{n-1,n}^T & \gamma_n \end{pmatrix} \tag{14}$$

where diagonal elements γ_n consists of $\gamma_{i,j} = \langle r_i r_j \rangle - \langle r_i \rangle \langle r_j \rangle$, and correspond to the reduced state of a respective mode, and off-diagonal elements σ - carry the information about intermodal correlations.

A Gaussian state is defined as such a state that its characteristic function is Gaussian:

$$\chi(\xi) = \mathrm{e}^{-\frac{1}{4}\xi^T\gamma\xi + id^T\xi} \tag{15}$$

The quantum vacuum state, coherent states, squeezed states and thermal states are typical Gaussian states and they constitute an important class of states in quantum optics that are in the heart of CV quantum information processing. A density operator is a positive (semi-)definitive operator ($\rho \geq 0$) with $\mathrm{Tr}\rho = 1$. If $\rho \ngeq 0$, it does not describe a physical state. In other words, not any real symmetric $2N \times 2N$ matrix can be a legitimate covariance of a quantum state as the states must respect the Heisenberg uncertain relation. The condition for a physical Gaussian state is given in terms of the covariance matrix as follows:

Matrix γ is the covariance matrix of a physical state if and only if $\gamma + i\Omega \geq 0$. A Gaussian state is pure if and only if $\det\gamma = 1$.

This is the only necessary and sufficient constrain γ has to fulfill to be a proper covariance matrix of a respective physical Gaussian state. Basically it is also a necessary condition (but not sufficient) for non-Gaussian states. The constraint generalizes the expression of Heisenberg uncertainty principle.

Single-mode Gaussian states can be completely characterized by the displacement operator and a 2×2 covariance matrix.

$$\gamma = \begin{bmatrix} a & c \\ c & b \end{bmatrix}$$

A general two mode Gaussian state is characterized by a mean $d = d_1 \otimes d_2$ and a covariance matrix

$$\gamma_{AB} = \begin{bmatrix} \gamma_A & C \\ C & \gamma_B \end{bmatrix}$$

where $\gamma_{A(B)}$ are the covariance matrices of the the two modes, and C is the matrix that describes the correlation between two modes.

The case where $C = 0$ corresponds to a tensor product of single-mode states:

$$\gamma_{AB} = \gamma_A \oplus \gamma_B$$

Previous definitions can be generalized to systems of N modes.

2.2.1 Vacuum, Coherent and Thermal states

The vacuum state is the state with lowest possible energy. Generally it contains no physical particles. It is not however some absolutely empty void, it contains fleeting electromagnetic waves and transient fluctuation that exhibits many of the characteristics of an ordinary particle, but that exists for a limited time. It means that although the average values of the fields vanish in a quantum vacuum, their variances do not. The vacuum state is a state centered at the origin of the phase space ($D = (0, 0)$) with a covariance matrix $\gamma = \mathbb{I}$.

Coherent state is a displaced vacuum state. It also holds some of the vacuum state properties like minimum uncertainty and identity covariance matrix with a non-zero displacement vector $D = (d_x, d_p)$.

$$|\alpha\rangle \equiv D(\alpha)\,|0\rangle \equiv \mathrm{e}^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}\,|0\rangle \tag{16}$$

The coherent state is an eigenstate of the non-Hermitian annihilation operator $\hat{a}$, and it can be expressed as a superposition of eigenstates of the radiation field.

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{17}$$

Coherent states are the most appropriate quantum representation of what we might call classical light (there is, of course, no such thing as classical light, but coherent states with a large number of photons are closest to what we imagine classical light should be)[17].

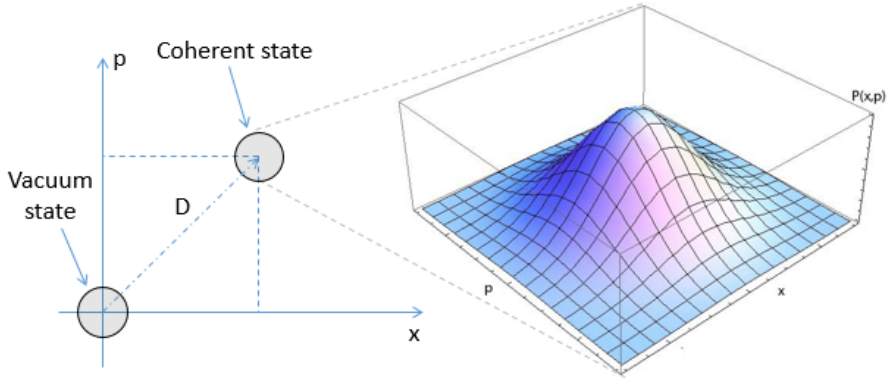

Figure 6: Vacuum and coherent states on phase space.

The thermal state has null mean value and covariance matrix

$$\gamma = \begin{bmatrix} V & 0 \\ 0 & V \end{bmatrix}$$

The quantity V can be expressed in terms of the average number of photons n contained in the thermal state as $V = 2n + 1$. The vacuum can be seen as a thermal state which contains no photons at all ($n = 0$).

Thermal state can generalized as a case of a noisy version of coherent state.

2.2.2 Squeezed state

The mathematical features of a quadrature squeezed state are given, where the uncertainty of one quadrature component is forced to be smaller than that of the

conventional minimum uncertainty; however, it is accompanied by an increase in the fluctuation of the other component. The squeezed state is obtained by first squeezing the vacuum and then displacing it. The degree of attenuation of one quadrature and simultaneous amplification of another is determined by r, which is called the squeezing factor[18]. The squeezed vacuum state has similarly to vacuum state null mean value. However its covariance differs from identity and can be written as

$$\gamma = \begin{bmatrix} \mathrm{e}^{-2r} & 0 \\ 0 & \mathrm{e}^{2r} \end{bmatrix}, \tag{18}$$

where one can observe that the uncertainty among one quadrature is squeezed (x if $r > 0$ and p if $r < 0$) and anti-squeezed among the conjugate one. Squeezed coherent states have exactly the same covariance matrix but with a non null displacement.

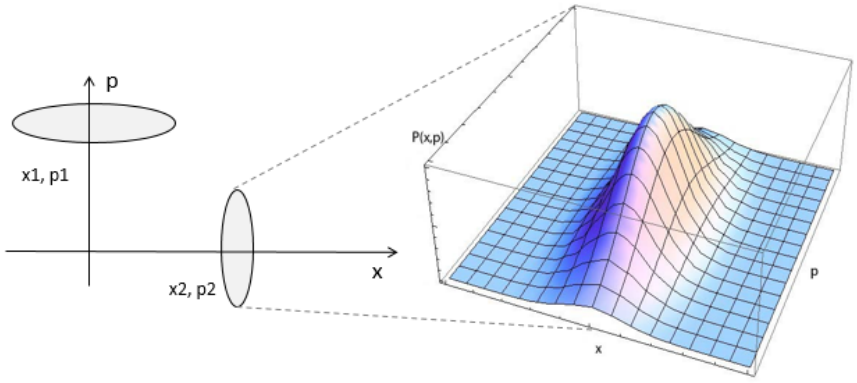

Figure 7: Squeezed states

The two-mode squeezed vacuum states is a key resource for a practical implementation of CV quantum key distribution, playing an equivalent role as Bell pairs ($(|00\rangle + |11\rangle)/\sqrt{2}$) in qubit quantum information. Its mean is null and its covariance matrix reads,

$$\gamma_{EPR} = \begin{bmatrix} \cosh 2r\mathbb{I} & \sinh 2r\sigma_z \\ \sinh 2r\sigma_z & \cosh 2r\mathbb{I} \end{bmatrix}, \tag{19}$$

where

$$\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Notice that tracing one mode leaves the other mode in a thermal state of a variance $\cosh(2r) = 2n + 1$.

As for the one mode case one can transform any two-mode Gaussian state in a two-mode thermal state by applying a given sequence of operations[19].

2.3 Continuous-Variable Quantum Key Distribution

The discrete modulation of quantum states as in BB84 stems fairly naturally from the need to produce zeroes and ones for the final secret key. But since secret-key distillation can also process continuous key elements, in fact, continuous-variable protocols are fairly elegant alternatives to their discrete counterparts and allow for high secret key rates.

2.3.1 A protocol with squeezed states

Squeezed-states protocol is based on Alice preparing x (or p)-squeezed states displacing along x (or p), giving a thermal state of variance V as average output state. If Alice starts from an x-squeezed vacuum state with covariance matrix (equation (18)), then she encodes a random Gaussian distributed variable a (centered on zero and with variance V_A) into the x-displacement applied to the squeezed vacuum state ($d(0;0) \rightarrow (a,0)$). Averaging over all possible realizations we get the mixed Gaussian state with null mean value and covariance matrix

$$\gamma_s = \begin{bmatrix} \mathrm{e}^{-2r} + V_A & 0 \\ 0 & \mathrm{e}^{2r} \end{bmatrix} \tag{20}$$

We observe that by imposing $e^{-2r} + V_A = e^{2r}$ we obtain a thermal state of variance $V = e^{2r}$. This thermal state is indistinguishable from a thermal state realized by a mixture of p-squeezed states (squeezing parameter r) with Gaussian-distributed p-displacement (variance V_A)

$$\gamma_s = \begin{bmatrix} \mathrm{e}^{2r} & 0 \\ 0 & \mathrm{e}^{-2r} + V_A \end{bmatrix} = \begin{bmatrix} V & 0 \\ 0 & V \end{bmatrix}$$

As in BB84 information is being encoded in two conjugate quadratures with both output mixed states being the same thermal state of variance V , being then indistinguishable.

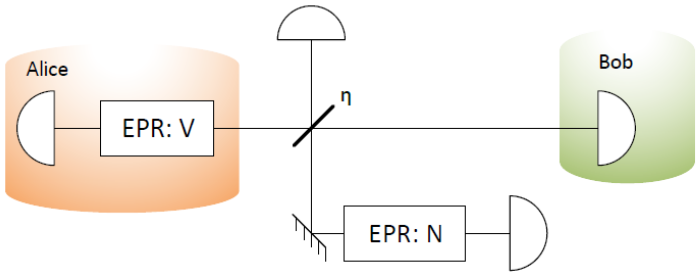

Figure 8: Squeezed state protocol QKD scheme

The quantum communication part of the protocol consists in repeating the following steps for each pulse sent by Alice:

1. First of all Alice generates a random number (a) from a Gaussian distribution of variance $V_A (V_A = \mathrm{e}^{2r})$ and a random bit (b) from a equiprobable binary distribution. At the same time Bob generates a random bit (b').

2. Depending on the value of the random bit (b) Alice sends a x-squeezed state with first moment $d = (a, 0)$ or a p-squeezed state with first moment $d = (0, a)$, where the squeezing r satisfies $V_A = 2 \sinh 2r$.

3. Bob, depending on his random bit ($b^{'}$), measures either x or p.

After Bob has measured all the pulses, the two partners proceed with the post-processing, which starts by applying sifting:

1. Alice discloses for each pulse the value of b (whether she displaced x or p).

2. Bob keeps only the cases where he measured the right quadrature ($b = b^{'}$).

Finally Alice and Bob apply a reconciliation protocols being a combination of discretization and error correction. The reconciliation protocols is followed by a privacy amplification protocol that extracts the secret key using a given hashing function, see [20] for more details on the post-processing.

During crucial step of reconciliation Alice and Bob use classical communications to extract a common key from their correlated elements, revealing as little information as possible to a third party and ignoring these key elements [21]. There are two main options for doing reconciliation:

Direct reconciliation (DR) . Alice sends correction information and Bob corrects his obtained key elements, so he will have the same values as Alice does. Basically Bob is reconstructing what was sent by Alice, and classical information has the same flow direction as quantum - from Alice to Bob.

Reverse reconciliation (RR). It this case classical information is being send from Bob to Alice, and Alice corrects her key elements to have the same values as Bob does. Alice adapts herself to what was received by Bob.

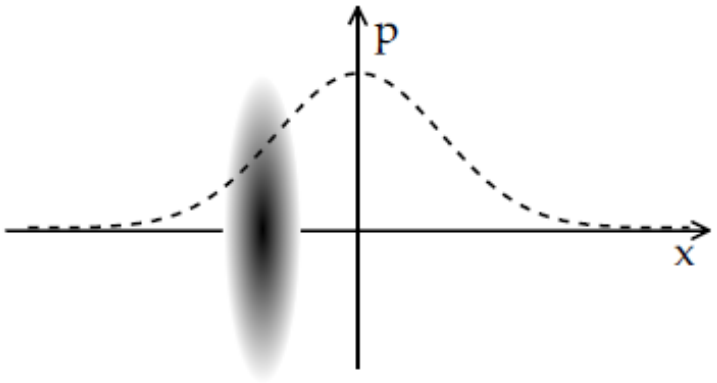

Figure 9: Alice generates x-squeezed vacuum states (squeezing $1/V$) and displaces them according to a Gaussian distribution (variance $V_A = V - 1/V$). The mixture is equivalent to a thermal state of variance V.

Yet, the production of squeezed states is rather difficult. The use of coherent states, much simpler to produce, is more practical. Even though coherent states are particular cases of squeezed states, decreasing the squeezing [15] makes the secret key rate go to zero. The solution was found by Grosshans and Grangier, who designed the first protocol, the so called GG02 protocol, where coherent states are modulated in both quadratures simultaneously [16]. It also uses the idea of the Gaussian modulation: Alice generates coherent states of a light mode with Gaussian-distributed quadratures, and Bob's measurements are homodyne measurements. This protocol allows for facilitated implementations and high secret-key generation rates [22]; this follows from the fact that homodyne detection can operate faster than the photon detectors used for BB84.

2.3.2 A protocol with coherent states

In the standart GG02 protocol, Alice encodes two different key elements, one of which will be discarded by Bob. The idea is that a thermal state of variance V can also be obtained by a bi-variate Gaussian mixture of coherent states. Alice encodes a random bi-variate Gaussian-distributed variable (a_x, ap) (centered on zero and with variance V_A) into the (x, p)-displacement applied to the vacuum:

$$\gamma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \rightarrow \gamma_c = \begin{bmatrix} V_A + 1 & 0 \\ 0 & V_A + 1 \end{bmatrix}$$

By imposing $V_A = V - 1$ we obtain after averaging over the outgoing pulses a thermal state of variance V, as shown in figure 10.

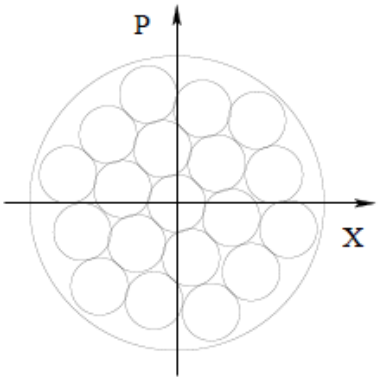

Figure 10: Alice generates coherent states with a random mean value (a_x, a_p) according to a Gaussian distribution (variance V_A). The mixture is equivalent to a thermal state ($V = V_A - 1$).

The protocol BB84 and the squeezed-state protocol both rely on the sifting of uncorrelated measurements. This protocol is different in the sense that no quantum state is discarded, but instead two pieces of information are encoded, one of which is discarded. As in previously described protocol Alice repeats next steps for each sended pulse:

1. Alice generates two random real numbers (a_x, a_p) from two independent Gaussian distributions of variance $V_A (V_A = V - 1)$ and Bob generates a random bit b.

2. Alice sends a coherent state centered in $d = (a_x, a_p)$ to Bob.

3. Bob depending on his random bit (b), measures either x or p.

After Bob has received all the pulses, he and Alice proceed with the post-processing, which starts by applying sifting:

1. Bob discloses value of b for each measurement (whether he measured x or p quadrature).

2. Alice and Bob keep $a_x$or a_p, depending on the value of b and discard the other quadrature.

After the sifting, they proceed with reconciliation and privacy amplification algorithms in order to obtain a secret key.

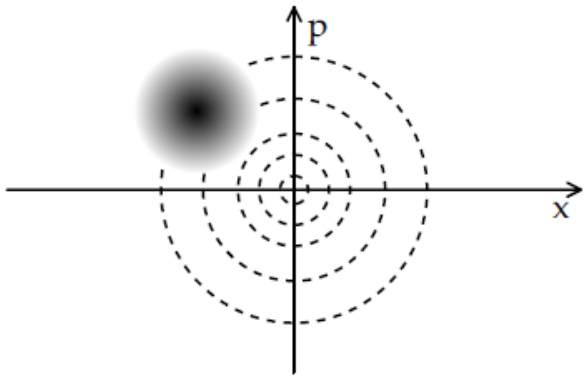

Figure 11: Schematic description of the encoding. The coherent states, such as the one illustrated in the upper left quadrant, are modulated along both axes. Their centers follow a bivariate Gaussian distribution, illustrated by the concentric circles.

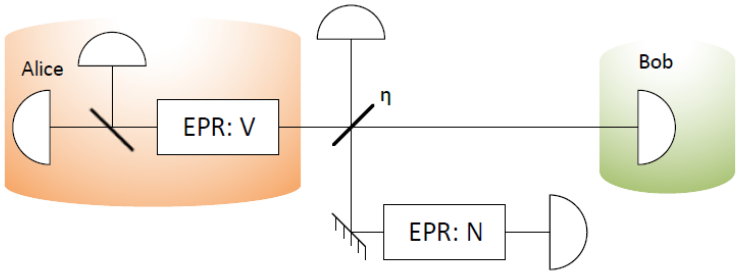

Figure 12: Coherent state protocol QKD scheme

In this protocol Alice generates two random real numbers but uses only one to generate the secret key. Interestingly, one can modify the coherent states protocols[16] in order to use both values, as shown in [23]. The idea is to replace Bob homodyne measurement by an heterodyne detection, where the incoming beam is divided in two using a balanced beamsplitter and measure x on one and p on the other using homodyne detection, this protocol is called *no basis switching protocol*.

2.4 Homodyne detection

Homodyne detection has been a powerful method for measuring phase sensitive properties of traveling optical fields which are suitable for quantum-state reconstruction, and a number of sophisticated detection schemes have been studied.

In the four-port basic scheme, a signal field is combined, through a lossless beam splitter, with a highly stable reference field which has the same mid-frequency as the signal field. The reference field, also called local oscillator, is usually prepared in a coherent state of large photon number. The superimposed fields impinge on photodetectors, the numbers of the emitted (and electronically processed) photoelectrons being the homodyne detection output (for the basic ideas, see [24, 25, 26]). The observed interference fringes, which vary with the difference phase between the two fields, reflect the quantum statistics of the signal field and can be used – under certain circumstances – to obtain the quantum state of the signal field. The homodyne output can be fully given in terms of the joint-event probability distribution of the detectors in the output channels. In balanced homodyning, difference-event distributions are measured. In particular, the difference-event statistics measurable by a perfect four-port homodyne detector directly yields the quadrature-component statistics of the signal field, which has offered novel possibilities of quantum-state measurement.

Our basic detection instrument is the balanced homodyne detector. Homodyne detector consists of a 50:50 beam splitter, two photodetectors, a reference beam having a well-defined phase with respect to the signal field, and electronic circuit.

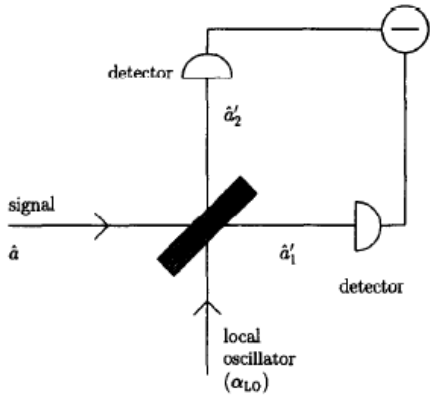

Figure 13: Balanced homodyne detector. The signal is optically mixed with a strong coherent local oscillator using a 50:50 beam splitter. The emerging fields are detected and the photocurrents are electronically subtracted to yield the measured quantity.

The signal and the reference beam (also called "local oscillator") are optically mixed at the beam splitter. The merging beams are detected and measure photocurrents are electronically subtracted to yield the measured quantity

$$\triangle \hat{J} = \hat{a'}_2^\dagger \hat{a'}_2 - \hat{a'}_1^\dagger \hat{a'}_1 = \frac{1}{2}\left(\hat{a}^\dagger + \hat{a}_{LO}^\dagger\right)(\hat{a} + \hat{a}_{LO}) - \frac{1}{2}\left(\hat{a}^\dagger - \hat{a}_{LO}^\dagger\right)(\hat{a} - \hat{a}_{LO}) = \\ = \hat{a}^\dagger \hat{a}_{LO} + \hat{a}\hat{a}_{LO}^\dagger. \quad (21)$$

When the local oscillator is coherent and intense with respect to the signal we may describe it classically. We simply substitute the annihilation operator $\hat{a}_{LO}$ by the complex amplitude α_{LO}:

$$\hat{a}_{LO} \to \alpha_{LO} = |\alpha_{LO}| \, \mathrm{e}^{i\theta} \quad (22)$$

and obtain for the photocurrent difference

$$\triangle \hat{J} = |\alpha_{LO}| \left(\hat{a}\mathrm{e}^{-i\theta} + \hat{a}^\dagger \mathrm{e}^{i\theta}\right). \quad (23)$$

(A more refined quantum-statistical theory of homodyne detection can be found in [27, 28, 29]. However the later equation (23) simple formula remains correct for a local oscillator in a highly excited coherent state.) Hence the balanced homodyne detector measures a quadrature component

$$\triangle \hat{J} = |\alpha_{LO}| \sqrt{2} \cdot \hat{x}_\theta \quad (24)$$

i.e. any linear combination of *position* $\hat{x} \equiv \hat{x}_0$ and *momentum* $\hat{p} \equiv \hat{p}_{\pi/2}$ corresponding to a rotation $\hat{x}(\Theta) = \hat{x}\cos\Theta + \hat{p}\sin\Theta$. The rotation angle is defined by the local oscillator phase Θ (or, to be more precise, by the phase difference between local oscillator and signal). Shifting this phase varies the mixing angle between *position* and *momentum*. Thus homodyne detection drastically enlarges our measuring capabilities in a relatively simple way.

3 Entropy and information

3.1 Shannon entropy

Entropy is a key concept of information theory. It measures how much uncertainty there is in the state of a physical system. The key concept of classical information theory is the *Shannon entropy*. Suppose we learn the value of a random variable X. The Shannn entropy of X quantifies how much information we gain, on average, when we learn the values of X. An alternative view is that the entropy of X measures the amount of *uncertainty* about X before we learn its value. These two viewers are complementary; we can view the entropy either as a measure of our uncertainty *before* we learn the value of X, or as a measure of how much information we have gained *after* we learn the value of X.

Intuitively, the information content of a random variable should not depend on the labels attached to the different values that may be taken by the random vriable. For example, we expect that a random variable taking the values "heads" and "tails" with respective probabilities 1/4 and 3/4 contains the same amount of

information as a random variable that takes the values 0 and 1 with respective probabilities 1/4 and 3/4. For this reason, the entropy of a random variable is defined to be a function of the probabilities of the different possible values the random variable takes, and is not influenced by the labes used for those values. We often write the entropy as a function of a probability distribution, $p_1, \cdots, p_n$. The Shannon entropy associated with this probability distribution is defined by

$$H(X) \equiv H(p_1, ..., p_n) \equiv -\sum_x p_x \log p_x. \tag{25}$$

Note that in the definition logarithms indicated by "log" are taken to the base two. It is conventional to say that entropies are measured in "bits" with this convention for the logarithm. What about the situation when $p_x = 0$, since $\log 0$ is undefined? Intuitively, an event which can never occur should not contribute to the entropy, so by convention we agree that $0 \log 0 \equiv 0$. More formally, $\lim_{x \to 0} x \log x = 0$, which provides further support for convention [30].

The *relative entropy* is a very useful entropy-like measure of the closeness of two probability distributions, $p(x)$ and $q(x)$, over the same index set, x. For these distributions it can be defined by

$$H(p(x) || q(x)) \equiv \sum_x p(x) \log \frac{p(x)}{q(x)} \equiv -H(X) - \sum_x p(x) \log q(x). \tag{26}$$

The relative entropy is non-negative, $H(p(x) || q(x)) \geq 0$, with equality if and only if $p(x) = q(x)$ for all x. The relative entropy is often useful, not in itself, but because other entropic quantities can be regarded as special cases of the relative entropy.

The joint entropy of two random variables X and Y is defined as,

$$H(X, Y) = -\sum_{x,y} p(x, y) \log p(x, y) \tag{27}$$

and may be extended to any vector of random variables. The joint entropy measures total uncertainty about the pair(X, Y). The remaining uncertainty about the pair (X, Y), is associated with remaining lack of knowledge about X, even given that we know Y. The entropy of X conditional on knowing Y is therefore defined by

$$H(X|Y) \equiv H(X, Y) - H(Y). \tag{28}$$

The *conditional entropy* is a measure of how uncertain we are, on average, about the value of X, given that we know the value of Y.

A second quantity, the mutual information content of X and Y, measures how much information X and Y have in common. Suppose we add the information content of X, $H(X)$, to the information content of Y. Information which is common to X and Y will have been counted twice in this sum, while information which is not common will have been counted exactly once. Subtracting

off the joint information $H(X,Y,)$, we therefore obtain the common or *mutual information* of X and Y:

$$H(X:Y) \equiv H(X) + H(Y) - H(X,Y) \tag{29}$$

Conditional entropy can be related to mutual information as

$$H(X:Y) = H(X) - H(X|Y) \tag{30}$$

The various relationships between entropies may mostly be deduced form the "entropy Venn diagram" shown in figure 14. Such figures are not completely reliable as a guide to the properties of entropy, but they provide a useful mnemonic for remembering the various definitions and properties of entropy.

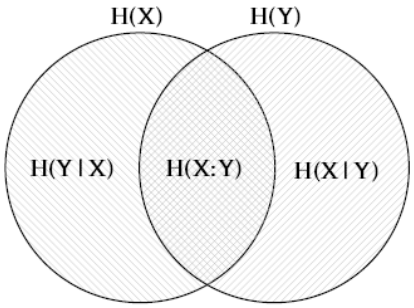

Figure 14: Relationships between different entropies.

Basic properties of Shannon entropy:

1. $H(X,Y) = H(Y,X)$, $H(X:Y) = H(Y:X)$.
2. $H(Y|X) \geq 0$ and thus $H(X:Y) \leq H(Y)$, with equality if and only if Y is a function of X, $Y = f(X)$.
3. $H(X) \leq H(X,Y)$, with equality if and only if Y is a function of X
4. **Subadditivity**: $H(X,Y) \leq H(X) + H(Y)$ with equality if and only if X and Y are independent random variables.
5. $H(Y|X) \leq H(Y)$and thus $H(X:Y) \geq 0$, with equality in each if and only if X and Y are independent random variables.
6. **Strong subadditivity**: $H(X,Y,Z)+H(Y) \leq H(X,Y)+H(Y,Z)$, with equality if and only if $Z \to Y \to X$ forms a Markov chain.
7. **Conditioning reduces entropy**: $H(X|Y,Z) \leq H(X|Y)$

3.2 Von Neumann entropy

The Shannon entropy measures the uncertainty associated with a classical probability distribution. Quantum states are described in a similar fashion, with density operators replacing probability distributions.

Von Neumann defined the entropy of a quantum state ρ by the formula

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho) \tag{31}$$

In this formula as in the case of Shannon entropy is taken to base two. If $\lambda_x$are the eigenvalues of ρ then Von Neumann's definition can be re-expressed

$$S(\rho) = -\sum_x \lambda_x \log \lambda_x \tag{32}$$

where again $0 \log 0 \equiv 0$, as of the Shannon entropy. It is easy to show that the Von Neumann entropy is minimal ($S(\rho) = 0$)when the state is pure $\rho = |\psi\rangle \langle\psi|$ and it is maximum ($S(\rho) = \log d$) when the state is maximally mixed $\rho = \mathbb{I}/d$.

As for the Shannon entropy, it is extremely useful to define a quantum version of the relative entropy. Suppose ρ and σ are density operators. The *relative entropy* of ρ to σ is defined by

$$S(\rho||\sigma) = \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma) \tag{33}$$

As with the classical relative entropy, the quantum relative entropy can sometimes be infinite. In particular, the relative entropy is defined to be $+\infty$ if the kernel of σ (the vector space spanned by the eigenvectors of σ with eigenvalue 0) has non-trivial intersection with the support of ρ (the vector space spanned by the eigenvectors of ρ with non-zero eigenvalue), and is finite otherwise. The non-negativity of quantum relative entropy is described by Klein's inequality:

The quantum relative entropy is non-negative ,

$$S(\rho||\sigma) \geq 0, \tag{34}$$

with equality if and only if $\rho = \sigma$.

Basic properties of Von Neumann entropy:

1. The entropy is non-negative. The entropy is zero if and only if the state is pure.

2. In a $d-$dimensional Hilbert space the entropy is at most $\log d$. The entropy is equal to $\log d$ if and only if the system is in the completely mixed state $\mathbb{I}/d$.

3. Suppose a composite system AB is in pure state. Then $S(A) = S(B)$.

4. Suppose p_i are probabilities, and the states ρ_i have support on orthogonal subspaces. Then

$$S\left(\sum_i p_i \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i). \tag{35}$$

5. **Joint entropy theorem**: Suppose p_i are probabilities, $|i\rangle$are orthogonal states for a system A, and ρ_i is any set of density operators for another system, B. Then

$$S\left(\sum_i p_i |i\rangle\langle i| \otimes \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i). \tag{36}$$

3.3 Holevo bound

The hidden nature of quantum information lies at the heart of the power of quantum computation and quantum information, and the accessible information captures in a quantitative way this hidden nature of quantum information. Unfortunately, no general method for calculating the accessible information is known; however, a variety of important bounds can be proved, the most important of which is the Holevo bound.

The Holevo bound is an exceedingly useful upper bound on the accessible information that plays an important role in many applications of quantum information theory.

Suppose Alice prepares a state ρ_x where $X = 0, ..., n$ with probabilities $p_0, ..., p_n$. Bob performs a measurement described by POVM elements $\{E_y\} = \{E_0, ..., E_m\}$ on that state, with measurement outcome Y. The Holevo bound states that for any such measurement Bob may achieve:

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x), \tag{37}$$

where $\rho = \sum_x p_x \rho_x$.

The Holevo bound is thus an upper bound on the accessible information. The quantity appearing on the right hand side of the Holevo bound is so useful in quantum information theory that it is given a name, the Holevo quantity, and is sometimes denoted χ.

Unfortunately the accessible information does not generally achieve the Holevo bound. One can see that in order to saturate the Holevo bound using product measurements the states ρ must have orthogonal support, which is not generally satisfied. Interestingly one can saturate the Holevo bound if we allow Bob to apply collective measurements, which are more general than product measurements.

4 Security

Let us briefly recapitulate the security of the Gaussian CV QKD protocols. Even if most of the experimental implementations are based on prepare-and-measure schemes, the theoretical analysis mostly is done using an entanglement-based scheme, as they are completely equivalent [31] but latter significantly simplifies calculations or makes them possible in principle.

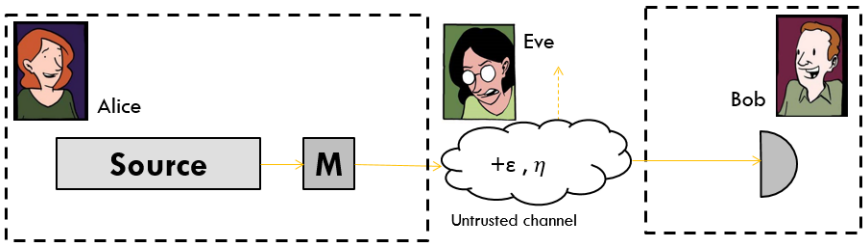

Figure 15: Prepare-and-measure protocol scheme

Prepare-and-measure protocol is straightforward - Alice uses radiation from a source (laser or optical parametric oscillator) and modulator on her side to encode the information into quantum states and than sends them through untrusted quantum channel where states suffer from losses (η) and excess noise (ϵ) and finally arrive to Bob's side.

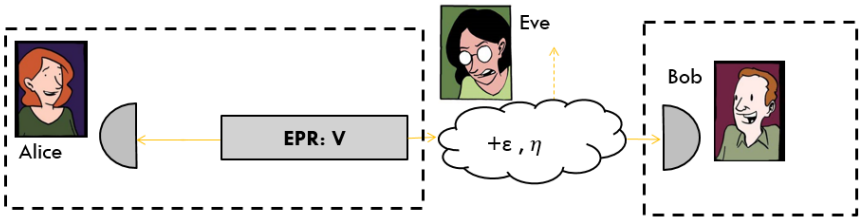

Figure 16: Entanglement-based protocol scheme based on squeezed states. For coherent states heterodyne measurement on Alice's side should be used.

In entanglement-based scheme Alice on her side generates an entangled state, sends one mode to Bob and measures with appropriate basis the other mode. Alice can vary her measurements from heterodyne to homodyne depending on which states she wants to use during QKD, coherent or squeezed states respectively.

4.1 Individual attacks

Individual attacks are those in which Eve is restricted to interact with and measure each transmitted signal independently. It was proven [32] that Gaussian individual attacks are optimal against Gaussian direct and reverse reconciliation protocols. Since Alice and Bob apply only Gaussian measurements that do not mix x and p quadratures, and their mutual information is fixed by the amount of data that was obtained by both of them and the efficiency of reconciliation, in order to hold an optimal attack Eve should apply a Gaussian map. Therefore, Alice and Bob before measurement share quantum state ρ_{AB} that is assumed to be a Gaussian two-mode state with 0 mean value and respective covariance

matrix γ_{AB}. Since neither Gaussian operations, nor noise in the Gaussian channel can introduce correlations between x and p quadratures, one can write a covariance matrix as

$$\gamma_{AB} = \begin{bmatrix} \gamma_{AB}^{x} & 0 \\ 0 & \gamma_{AB}^{p} \end{bmatrix} \tag{38}$$

Security is shown as the positivity of the key, following Csiszar - Korner theorem [10].

Key rates for direct reconciliation and reverse reconciliation can be written respectively as:

$$K_{DR} = I_{AB} - I_{AE}, \tag{39}$$

$$K_{RR} = I_{AB} - I_{BE}, \tag{40}$$

where I is mutual information (equation (29)) between respective parties. In terms of equation (30) key rates can be written as:

$$K_{DR} = H\left(A|E\right) - H\left(A|B\right), \tag{41}$$

$$K_{RR} = H\left(B|E\right) - H\left(B|A\right). \tag{42}$$

Since states and channel are Gaussian, entropies can be expressed in terms of conditional variances,

$$H\left(X|Y\right) = \frac{1}{2}\log V_{X|Y}, \tag{43}$$

where the log is to the base 2 and entropy is measured in bits, so the final result would give us quantity of bits per pulse.

Mutual information written in conditional variances:

$$I_{AB} = \frac{1}{2}\log\frac{V_B}{V_{B|A}} = \frac{1}{2}\log\frac{V_A}{V_{A|B}}, \tag{44}$$

and variances itself is:

$$V_{X|Y} = V_X - \frac{C_{XY}^2}{V_Y}, \tag{45}$$

where $V_{X(Y)}$- variance of a respective light mode and C_{XY} - correlation between those modes.

In order to have the most general case of the noisy quantum channel one should assume the Eve holds the purification of state ρ_{AB}. Using previously described entropies and Heisenberg equation one can write:

$$V_{A|E}V_{A|B} \geq 1 \tag{46}$$

which sets the bound on preciseness of Eve's possible measurements and allows to upper bound Eve's information in case of individual attacks. Equation (46) can also be written in terms of measured quadratures for different types of reconciliations, but general meaning stays the same.

4.1.1 Pure losses

Let us first consider a purely lossy channel. During calculations it was assumed that all other devices in schemes are ideal.

Expressions for mutual information between Alice and Bob, Alice and Eve and Bob and Eve can be respectively written as,

$$I_{ab} = \frac{1}{2}\log_2\left(\frac{V}{V - \frac{\eta(V^2-1)}{-\eta+\eta(k+V)+1}}\right) \tag{47}$$

$$I_{ae} = \frac{1}{2}\log_2\left(\frac{V}{V - \frac{(1-\eta)(V^2-1)}{\eta+(1-\eta)(k+V)}}\right) \tag{48}$$

$$I_{be} = \frac{1}{2}\log_2\left(\frac{1-\eta+\eta(k+V)}{1-\eta+\eta(k+V) - \frac{\sqrt{\eta(1-\eta)}(1-k-V)^2}{\eta+(1-\eta)(k+V)}}\right) \tag{49}$$

Graph representations of equations (47,48,49) are shown on figure 17.

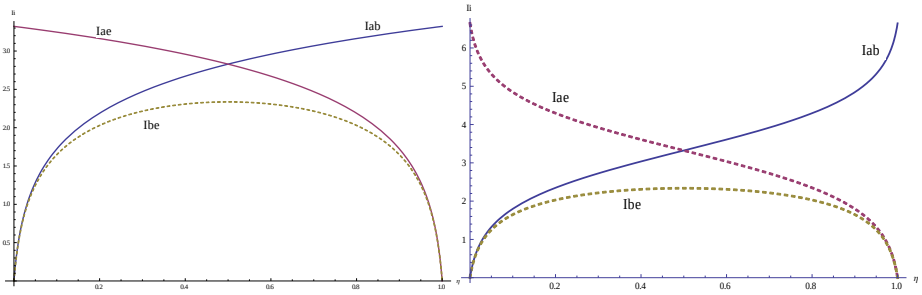

Figure 17: Dependencies of mutual information (left - coherent states protocol, right - squeezed state protocol) on channel losses,where I_{ab}, I_{ae}, I_{be}- mutual information between Alice and Bob, Alice and Eve, Bob and Eve respectively.

On figure 17 the behavior of mutual information between different protocol parties with decreasing of losses is shown. Losses should be apprehended as beam-splitter with corresponding transmittance η. It is easy to see that direct reconciliation becomes unsecure if $\eta < 0.5$, while reverse reconciliation can tolerate any pure loss.

4.1.2 Noisy channel

In order to saturate Eve's knowledge about the transferred key we have to take into account realistic conditions. One of these conditions is presence of noise in the untrusted channel. And since we make an assumption that Eve fully controls the losses and noise that quantum states suffer from, for calculations we use the so called entangling cloner [?] to purify Eve's attack. In an entangling cloner attack Eve possesses her own EPR source of variance N and a beamsplitter with transmittance η. Half of the Eve's state is mixed with Bob's mode on beamsplitter. Since Alice and Bob have access only to half of the EPR, they can see only thermal states with variance N. N is tuned in such a way to match the noise of the real channel. The other half of the EPR will serve to reduce Eve's uncertainty on the noise added by the channel. Since channel is Gaussian and phase-insensitive, noise affects x and p quadratures in a same way.

Eve has to fix N in a proper way:

$$N = \frac{\eta\varepsilon}{1-\eta} + 1. \tag{50}$$

In the most expedient scenario Eve has to store two ancillary systems E_1 and E_2, in two quantum memories and after Alice and Bob start to reveal the selected basis (key sifting) through classical channel, Eve will measure the right quadrature on systems E_1 and E_2. The correct measurement on E_2 will allow Eve to decrease the noise in E_1. Mutual informations for squeezed-state protocol after the whole process of key transferring, interaction with Eve's ancillas can be written as:

$$I_{AB} = \frac{\log\left(\frac{\eta V(V+\epsilon-1)+V}{\eta+\eta V(\epsilon-1)+V}\right)}{\log(4)} \tag{51}$$

$$I_{AE} = \frac{\log\left(\frac{V(\eta+\eta V(\epsilon-1)+V)}{\eta(V+\epsilon-1)+1}\right)}{\log(4)} \tag{52}$$

$$I_{BE} = \frac{\log\left(\frac{(\eta+\eta V(\epsilon-1)+V)(\eta(V+\epsilon-1)+1)}{V}\right)}{\log(4)} \tag{53}$$

On figure 18 one can we can see a difference between the squeezed state and coherent state protocols.

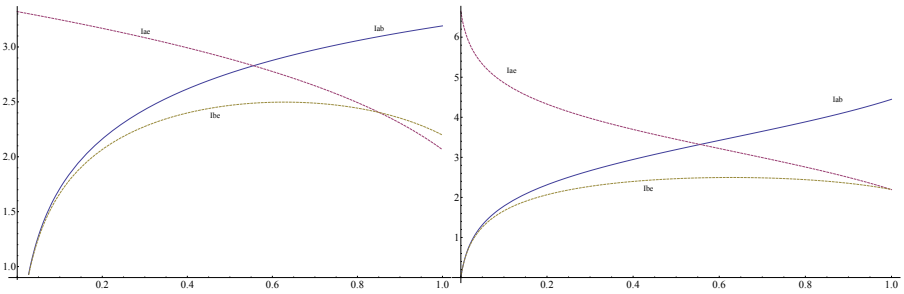

Figure 18: Mutual information on channel losses. Left - coherent state protocol, Right - squeezed state protocol, $\epsilon = 0.2$, $V = 100$

4.2 Collective attacks

Security of QKD protocols should be proven even for the case when Eve has no technological limitations, so she can achieve the Holevo bound equation (37). This case is generalized by collective attacks, security to which was shown to imply security against any attack. In this scenario key rates for direct and reverse reconciliations respectively read:

$$K_{DR} = I_{AB} - \chi_{AE}, \tag{54}$$

$$K_{RR} = I_{AB} - \chi_{BE}. \tag{55}$$

where $K_{DR(RR)}$depends on the key sifting, but does not depend on the purification ofρ_{AB}, and χ_{AE} (χ_{BE})- Holevo bound between respective parties.

Collective attacks are much more sophisticated attacks than individual ones. Eve's measurement is done after the processes of error-correction and privacy amplification are completed. During her attack Eve attaches a separate, uncorrelated probe to each transmitted state, than she keeps probes in a quantum memory (where quantum states can be kept for a long time) until she can gather additional information about error-correction and privacy amplification (eavesdropping a classical channel). After this Eve performs the optimal measurement on her probes in order to learn the maximal information on the final, sifted key. The case of collective attacks is the strongest attack suggested so far, and perhaps is the strongest possible attack.

During calculations of Holevo bound we use the fact that von Neumann entropies that are expressed through bosonic entropy functions:

$$S_X = \sum_n G\left(\frac{\lambda_n - 1}{2}\right), \tag{56}$$

where

$$G(x) = (x+1)\log(x+1) - x\log x. \tag{57}$$

For single-mode covariance matrix of Eve's state, key rate reads:

$$K_{DR(RR)} = I_{AB} - S_E + S_{E|A(E|B)} = I_{AB} - G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right), \quad (58)$$

where λ_n - symplectic eigenvalues of a respective covariance matrix.

Due to Williamson theorem [33] we know that for any N-mode covariance matrix γ there is a symplectic transformation S such that:

$$S\gamma S^T = \lambda \quad (59)$$

where λ is a tensor product of thermal states, called the Williamson normal form,

$$\lambda = \bigoplus_{k=1}^{N} \begin{bmatrix} \lambda_k & 0 \\ 0 & \lambda_k \end{bmatrix}. \quad (60)$$

The symplectic eigenvalues λ_k being the eigenvalues of the matrix $|i\Omega\gamma|$, where

$$\Omega = \begin{bmatrix} \omega & 0 \\ 0 & \omega \end{bmatrix}, \ \omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

The symplectic transformation is a unitary operation so a state is pure if and only if $\lambda = \mathbb{I}$. More precisely, the purity μ of a Gaussian state ρ of covariance matrix γ reads,

$$\mu = \mathrm{Tr}\rho^2 = \frac{1}{\sqrt{\det\gamma}}. \quad (61)$$

The determinant is then a symplectic invariant, as $\det S = 1$, which leads to,

$$\det\gamma = \det\lambda = \prod_{i=1}^{N} \lambda_i^2. \quad (62)$$

The easiest cases are for one and two mode covariance matrices. The normal decomposition of one mode: $\lambda_1 = \sqrt{\det\gamma_1}$.

For two mode covariance matrix

$$\gamma_{AB} = \begin{bmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB} & \gamma_B \end{bmatrix},$$

First symplectic invariant:

$$\det\gamma_{AB} = \lambda_1^2\lambda_2^2. \quad (63)$$

Second symplectic invariant:

$$\triangle = \lambda_1^2 + \lambda_2^2 = \det\gamma_1 + \det\gamma_2 + 2\det\sigma_{AB},$$

Then λ_i are given by $z^2 - \triangle z + \det\gamma_{AB} = 0$, $\lambda_{1,2} = \sqrt{z_{1,2}}$.

For bigger quantity of modes situation is much complicated and generally cannot be solved and simplified analytically [19].

5 Advanced security

5.1 Preparation noise

In ideal case when there are no losses and noise, and detectors are ideal, it is quite easy to obtain secure key between trusted parties. But for correct realistic calculations one should take into account all possible influences on quantum key distribution. Two of them were presented previously - channel losses η, that are modeled by a beamsplitter with respective transmittance, and excess noise ε. Detectors are typically assumed to be trusted - preparation and receiving of the states are completely secure, there is no information leakage to potential eavesdropper, but the noise can be added on the trusted side. However, it was shown that noise on the remote receiver side does not limit the security, but can even be useful in reverse reconciliation scenario [34]. On the other hand, trusted preparation noise can break the security of coherent-state protocol [35] already for the pure loss in the case of reverse reconciliation, but can be compensated with proper purification [36]. In our theoretical analysis we consider both coherent and squeezed state protocols.

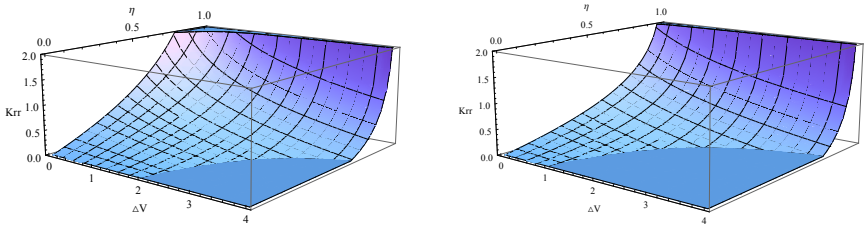

Figure 19: Dependency of key rate for reverse reconciliation on channel losses and preparation noise $\triangle V$ for squeezed (left) and coherent (right) state protocol.

One should emphasize that preparation noise, if it is on the refeence side of reconciliation, does not break the security [19, 37].

First, we generalize the study of the preparation noise to the squeezed state protocol [10]. For purely lossy channels in case of infinitely squeezed states expression for preparation noise that breaks the security can be written as,

$$\triangle V = \frac{2-\eta}{1-\eta} \tag{64}$$

and for coherent state protocol with arbitrary large source variance [35] it is known as more strict bound:

$$\triangle V = \frac{1}{1-\eta} \tag{65}$$

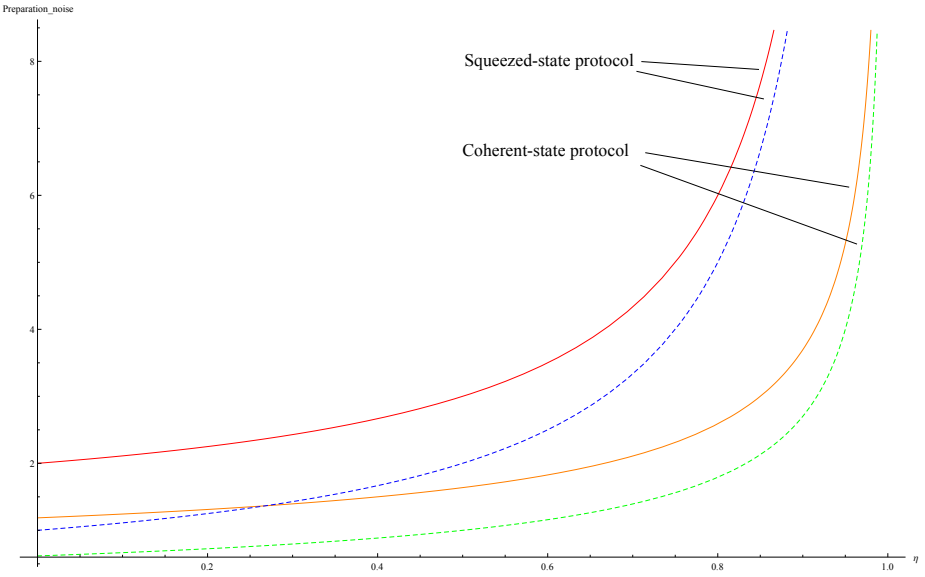

Figure 20: Comparison of dependencies of maximum tolerable preparation noise on channel losses between squeezed and coherent state protocols for purely lossy channel, for infinitely high variance $V \to \infty$ (solid) and mild variance $V = 2$ (dashed).

If the channel noise is present, then the expression for maximal tolerable preparation noise in case of entangling cloner attack on squeezed state protocol, reads

$$\triangle V = \frac{2 - \eta - \eta\epsilon^2 + 2\eta\epsilon - 2\epsilon}{1 - \eta + \eta\epsilon}. \tag{66}$$

As can be seen from figure 20 squeezed state protocol is more robust against the preparation noise upon the same energy of the signal states.

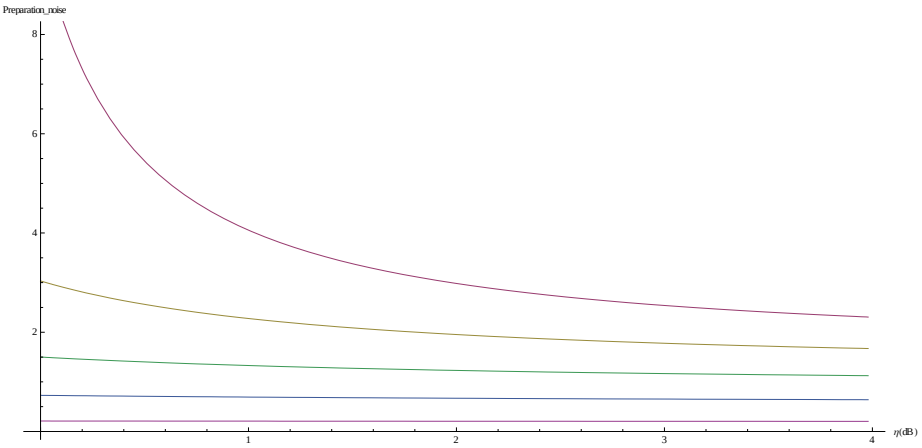

Figure 21: Dependency of preparation noise on channel losses (in dB) for various influences of excess noise ε, where starting from top curve $\varepsilon = 0.1, 0.3, 0.5, 0.7, 0.9$

5.2 Side channel

It is unrealistic to assume that attackers will attempt to directly take on the computational complexity of breaking the cryptographic primitives employed in security mechanisms. An interesting analogy can be drawn in this regard between strong cryptographic algorithms and a highly secure lock on the front door of a house. Burglars attempting to break into a house will rarely try all combinations necessary to pick such a lock; they may break in through windows, break a door at its hinges, or rob owners of a key as they are trying to enter the house. Similarly, almost all known security attacks on cryptographic systems target weaknesses in the implementation and deployment of mechanisms and their cryptographic algorithms. These weaknesses can allow attackers to completely bypass, or significantly weaken, the theoretical strength of security solutions. It is important to investigate all possible ways an eavasdropper can "backdoor" the protocols.

User's devices were previously assumed to operate as required for the QKD protocol. However, actual devices do not necessarily operate as required; moreover, they may allow unwanted leakage of information. This kind of information leakage due to device imperfections is called a *side channel* and side channels exist in all types of communications.

Side channel concept also allows to simplify the calculations for preparation and detection noise, since it is hard to characterize all possible sources of preparation and detection noise and instead of treating all these sources separately, it is easier to describe their total impact as an additional side-channel under Eve's control.

Side channels are widely discussed in classical cryptography and are directly connected to the so called side channel attacks. Side channel attack is any

attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms. For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Some side-channel attacks require technical knowledge of the internal operation of the system on which the cryptography is implemented, although others such as differential power analysis are effective as black-box attacks.

In classical cryptography there are lots of different classes of such attacks - such as timing, power monitoring , electromagnetic, acoustic etc. In all cases, the underlying principle is that physical effects caused by the operation of a cryptosystem (on the side) can provide useful extra information about secrets in the system, for example, the cryptographic key, partial state information, full or partial plain texts and so forth. The term cryptophthora (secret degradation) is sometimes used to express the degradation of secret key material resulting from side channel leakage [38]. Further we consider effect on side-channels in CV QKD.

5.2.1 Vacuum input

Let us consider the side-channel loss, where the input of a side-channel is just a vacuum state coupled to a signal with ratio S and is not by any means controlled by Eve (figure 22,(23)). However Eve can use this side channel to gain knowledge about the key without introducing errors. As can be seen from previous calculations reverse reconciliation is more robust for key transferring to longer distances and it also allows us to cross out the influence of detection noise, so further we will proceed with calculations only for reverse reconciliation.

First we calculate the impact of side channel on the security against individual attacks to estimate the insecurity region. As we perform the calculations in the equivalent entangled-based setup (using the reverse reconciliation), the expression for mutual information between Alice and Bob and Bob and Eve using equation (44) are

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}}\,, \tag{67}$$

$$I_{BE} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|E_1E_2}}\,, \tag{68}$$

where $V_{A|B} = V_A - \frac{C_{AB}^2}{V_B}$ and $V_{B|E_1E_2} = V_{B|E_1} - \frac{C_{BE_2|E_1}^2}{V_{E_2|E_1}}$ are relevant conditional variances (equation (45)), E_1 stands for the side channel and E_2 stands for channel losses. In our case, the variances are $V_A = V$ (or $V_A = \frac{V+1}{2}$ for coherent-state protocol), $V_B = \eta S(V-1)+1$, $V_{E_1} = S+V-SV$, $V_{E_2} = S(\eta - \eta V+V-1)+1$ and the mode correlations are $C_{AB} = \sqrt{\eta}\sqrt{S}\sqrt{V^2-1}$ (or $C_{AB} = \frac{\sqrt{\eta}\sqrt{S}\sqrt{V^2-1}}{\sqrt{2}}$ for coherent-state protocol), $C_{BE_1} = \sqrt{\eta}\left(-\sqrt{-(S-1)S}\right)(V-1)$, $C_{BE_2} = \sqrt{-(\eta-1)\eta}(-S)(V-1)$, $C_{E_1E_2} = \sqrt{1-\eta}\sqrt{-(S-1)S}(V-1)$.

In the limit of arbitrary large source variance (arbitrary high modulation) key rate for squeezed and coherent state protocols respectively turns to

$$K_{(S)RR} = \frac{\log\left(\frac{\eta S}{1-\eta S}\right) - \log\left[\eta S(1-\eta S)\right]}{\log(4)} \tag{69}$$

$$K_{(C)RR} = \frac{\log(\eta S) - \log\left[\eta S(1-\eta S)\right]}{\log(4)} \tag{70}$$

The explicit expression for the key rate in general case is obtainable analytically, but it is too lengthly.

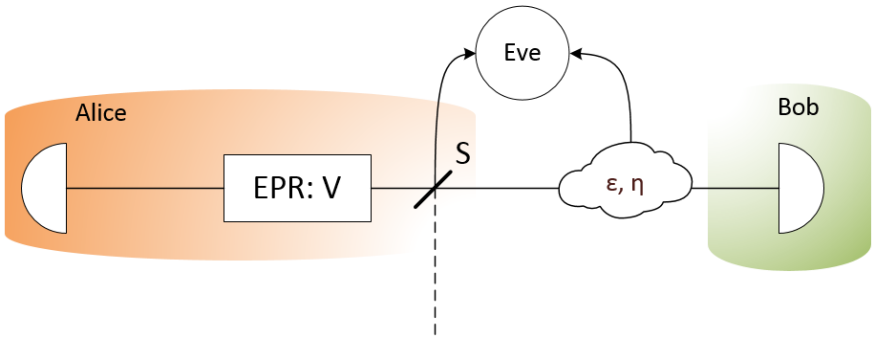

Figure 22: General EPR based quantum key distribution scheme with a side channel

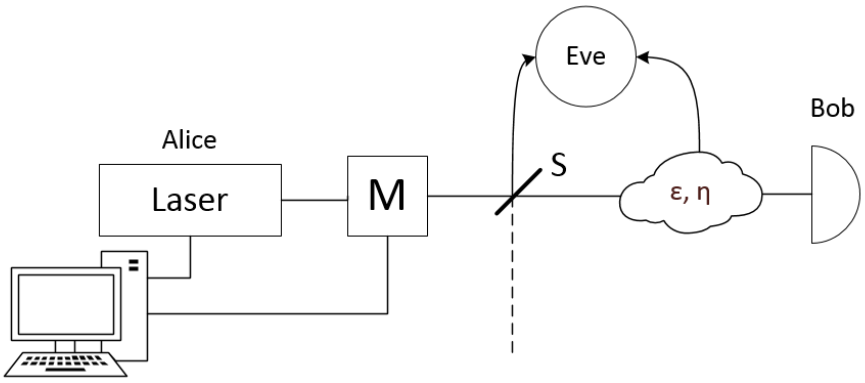

Figure 23: General Prepare & Measure based quantum key distribution scheme with a side channel

Since collective attacks are optimal and predict "worst case scenario" (in

other words if protocol is secure against them, than it is generally secure) in further we will proceed calculations for collective attacks.

In the case of collective attacks it is convenient to look at the influence of the side-channel noise on the robustness of protocols to factors that limit transmission distance, key rates etc., factors that cannot be affected by trusted parties. Channel losses η are usually related to transmission distances. One of the biggest limitations however is associated with excess noise. By definition, excess noise is the noise above the vacuum noise level associated with channel losses, and it is a major issue in continuous variables QKD.

As can be seen from figure 24 coherent state protocol is less robust to excess noise than squeezed state protocol.

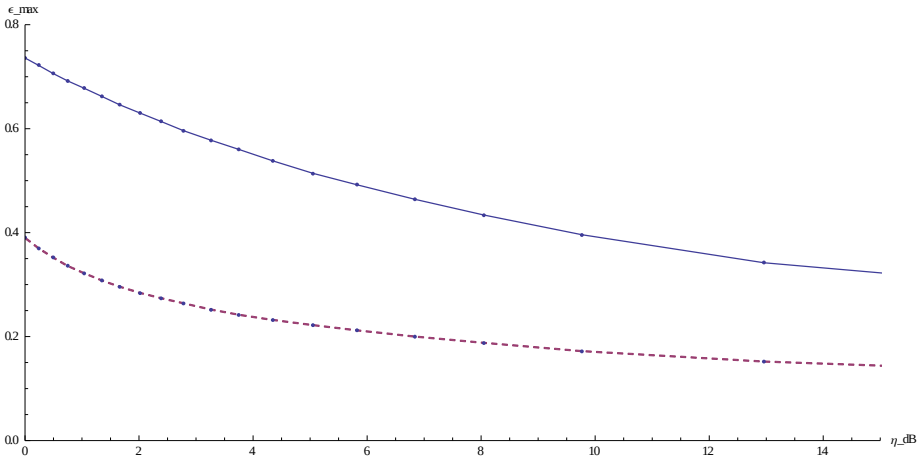

Figure 24: Comparison between coherent (dashed) and squeezed state protocols for maximum tolerable excess noise on channel losses (in dB) for absence of side-channel.

However side-channel decreases robustness of protocols to excess noise as seen from figure 25.

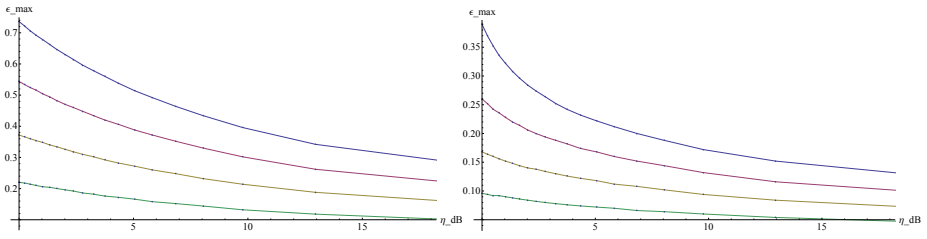

Figure 25: Side channel influence on coherent (left) and squeezed (right) state protocols for different coupling ratios (Starting from top $S = 1,\ 0.8,\ 0.6,\ 0.4$, where 1 stands for absence of side-channel)

5.2.2 Trusted input

Let us assume that the input of side channel is under Alice's control. In case of Prepare & Measure scheme, as seen on figure 26, Alice can use an additional modulator to input a known value of noise into the side channel. This side channel is coupled to a main signal with a coupling ratio S and its output is measured by Eve. It is assumed that Alice fully controls the side-channel modulator and Eve cannot by any means influence the input of the side-channel. Since Alice knows what noise she inputs into side channel, later she possibly can use this information to decrease Eve knowledge about the transmitted key.

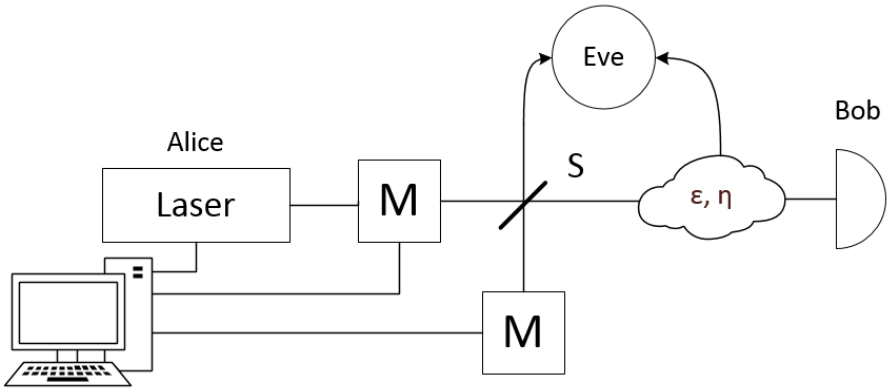

Figure 26: Prepare & Measure based side-channel quantum key distribution scheme with additional modulation input to side-channel

Alice's noise modulation will shift the input mode quadrature of side channel. We can write the input mode change in terms of x quadrature (calculations for the case when of p-quadrature is measured will be equivalent) as

$$x_0^{'} = x_0 + x_D \, ,$$

where x_D - shift, known to Alice, and its variance is reffered to as side-channel input noise (V_m), while x_0 - quadrature of a vacuum state with variance 1. Similarly, the same shift is applied to Alice's mode:

$$x_A^{'} = x_A + x_D \, ,$$

where x_A - quadrature of Alice's mode with a respective variance V. For individual attacks calculations are done similarly to previous case of vacuum side channel input. Variances for respective modes can be written as: $V_A = V + V_m$ (or $V_A = \frac{1}{2}(V + V_m + 1)$ for coherent-state protocol), $V_B = \eta S(V - V_m - 1) + \eta V_m + 1$, $V_{E_1} = V + S(1 - V + V_m)$, $V_{E_2} = \eta + (1-\eta)(S(V - V_m - 1) + V_m + 1)$ and the mode correlations are $C_{AB} = \sqrt{\eta}\left(\sqrt{S}\sqrt{V^2 - 1} + \sqrt{1 - S}V_m\right)$ (or $C_{AB} =$

$\frac{\sqrt{\eta}\left(\sqrt{S}\sqrt{V^2-1}+\sqrt{1-S}\mathrm{Vm}\right)}{\sqrt{2}}$ for coherent-state protocol), $C_{BE_1} = \sqrt{\eta}\sqrt{-(S-1)S}(1-V+V_m)$, $C_{BE_2} = \sqrt{-(\eta-1)\eta}(-(S(V-V_m-1)+V_m))$, $C_{E_1E_2} = \sqrt{1-\eta}\sqrt{-(S-1)S}(V-V_m-1)$.

In the limit of arbitrary large source variance (arbitrary high modulation) key rate for squeezed and coherent state protocols respectively turns to

$$K_{(S)RR} = \frac{\log\left(\frac{\eta S}{\eta\left(V_m-2\sqrt{-(S-1)S}V_m-S\right)+1}\right) - \log\left(\frac{\eta S(1-\eta(S+V_m)+V_m)}{V_m+1}\right)}{\log(4)} \quad (71)$$

$$K_{(C)RR} = \frac{\log\left(\frac{\eta S}{-2\eta\sqrt{-(S-1)S}V_m+\eta V_m+1}\right) - \log\left[-\frac{\eta S(\eta S+(\eta-1)V_m-1)}{V_m+1}\right]}{\log(4)} \quad (72)$$

As was mentioned previously EPR scheme is completely equivalent to P&M scheme. Corresponding EPR scheme to P&M scheme on figure 26 is shown on figure 27.To purify modilation, introduced by Alice, we add additional EPR source under Alice's control. This source with its own variance should be correlated with both modes of the original EPR source. The process goes as follows: second EPR source radiates a pair of entangled modes, one of the modes is sended directly into the side channel, the input of which is a vacuum state, and after this Bob's mode "interacts" with a side channel that is coupled to it with ratio S. The other entangled mode radiated from the second EPR source goes to Alice's side that and is coupled to her mode of the main EPR source.

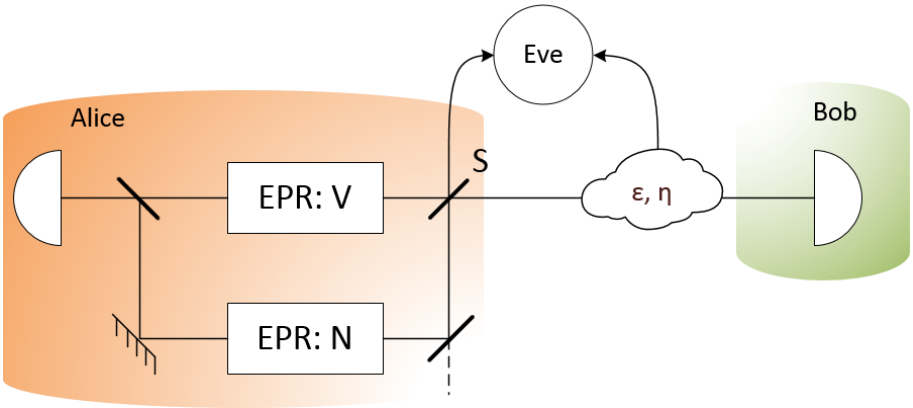

Figure 27: EPR based side-channel quantum key distribution scheme

Calculations of influence of the side-channel input noise on coherent and squeezed state protocols showed that the security of both of these protocols holds.

Let us first show maximal tolerable excess noise for both protocols. Basically the area below the dependancy curve is the area of a positive key rate and secure protocol. As can be seen on figure 28 - squeezed state protocol is much more robust to noise than the coherent state protocol. Since coherent-state protocol can be seen as more noisy version of squeezed-state protocol, the difference in robustness is understandable. Interesting to notice that the influence of side-channel input noise on exces noise is not linear. The robustness of both protocols starts from the respective values, increases and rapidly saturates. For this particular case coupling ratio ($S = 0.9$) is rather small which means that the side channel is only slightly "present".

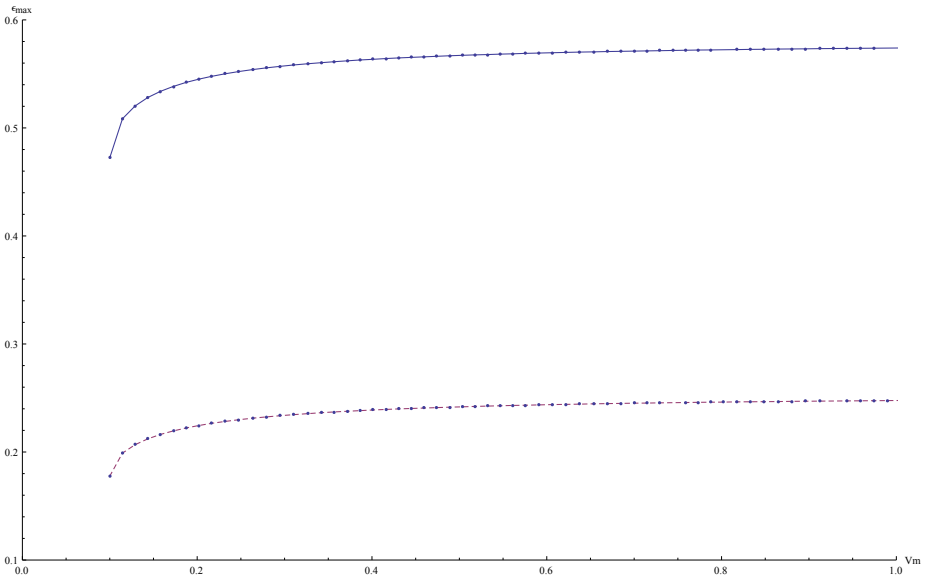

Figure 28: Dependency of maximal tolerable excess noise on side channel input noise for coherent (dashed) and squeezed state protocols. Side channel coupling ratio $S = 0.9$, $V = 1000$, $\eta = -3$dB.

Further calculations show that side-channel input noise can actually have positive impact on security of quantum key distribution. The behaviour of dependancy of key rate on side-channel input noise is similar to the dependancy of maxium tolerable excees noise on side-channel input noise. Turns out that protocol key rate is not linearly dependent on side channel input noise and for any value of excess noise and channel losses there is a respective maximum achievable key rate. The most interesing is that the key rate increases at first, this allows us to suggest that there is an optimal value of side-channel input noise that can partly compensate the influence of presence of side channel.

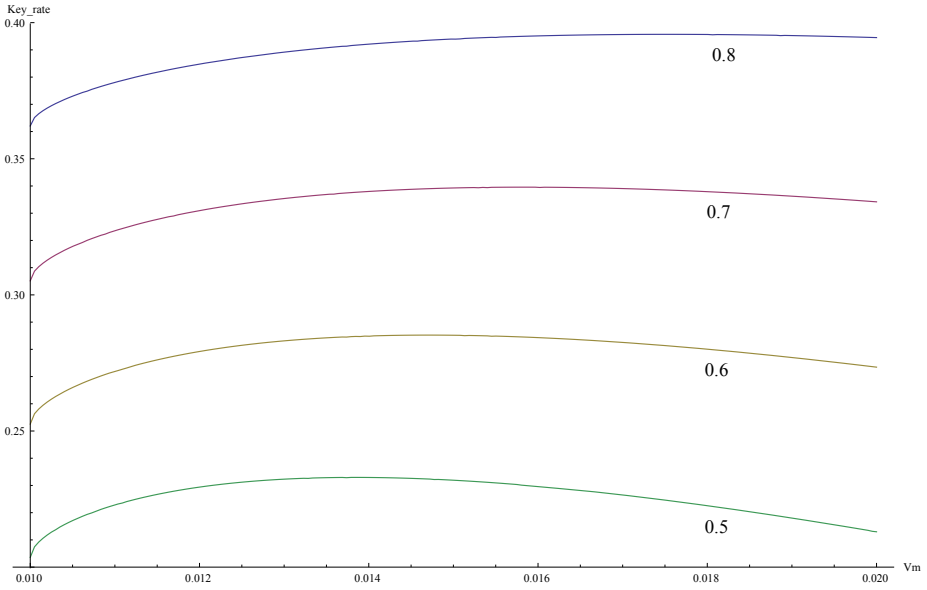

Figure 29: Coherent state protocol key rate depending on side-channel input noise for different side channel coupling ratios S. $V = 1000,\ \epsilon = 0,\ \eta = -3\text{dB}$

The same effect can be seen for squeezed state protocol.

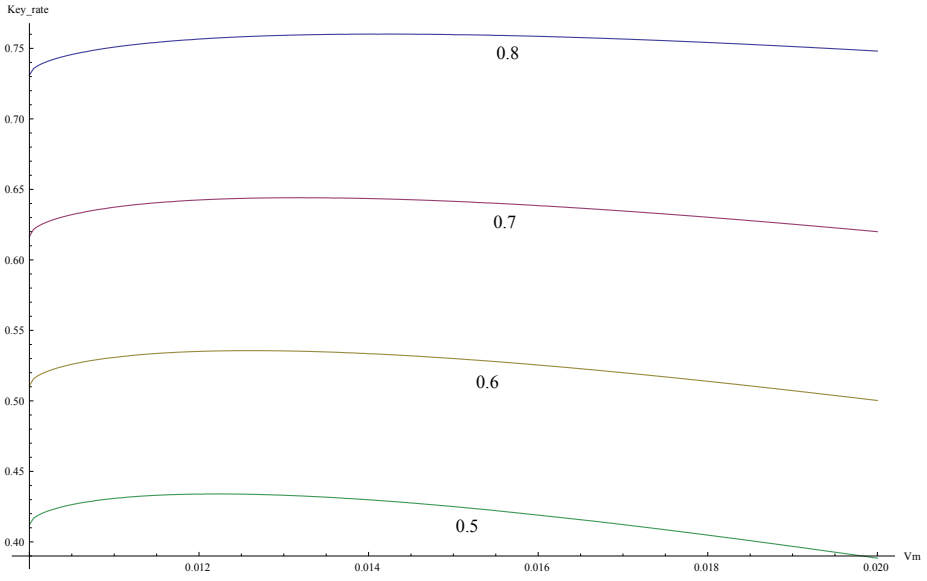

Figure 30: Squeezed state protocol key rate depending on side-channel input noise for different side channel coupling ratios S. $V = 1000,\ \epsilon = 0,\ \eta = -3\text{dB}$.

This dependency behavior remains similar for protocol robustness to excess noise.

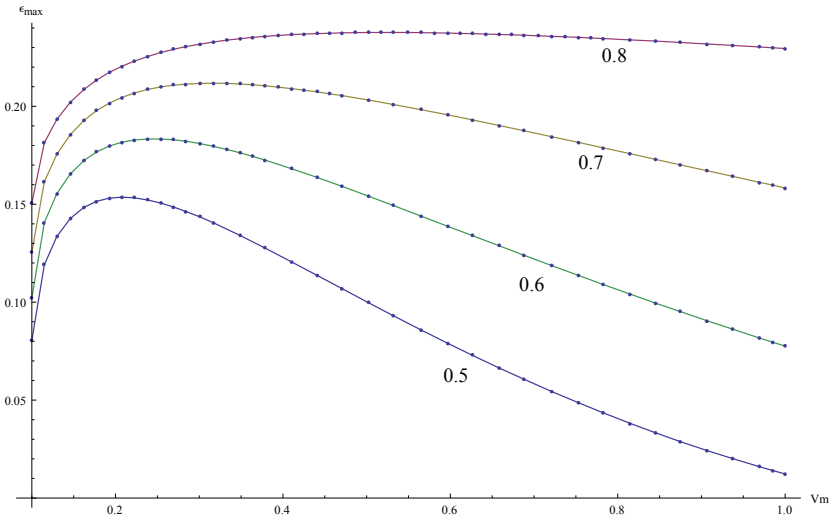

Figure 31: Dependency of maximal tolerable excess noise on side-channel input noise for coherent state protocol for various coupling ratios S, $V = 1000$, $\eta = -3$dB

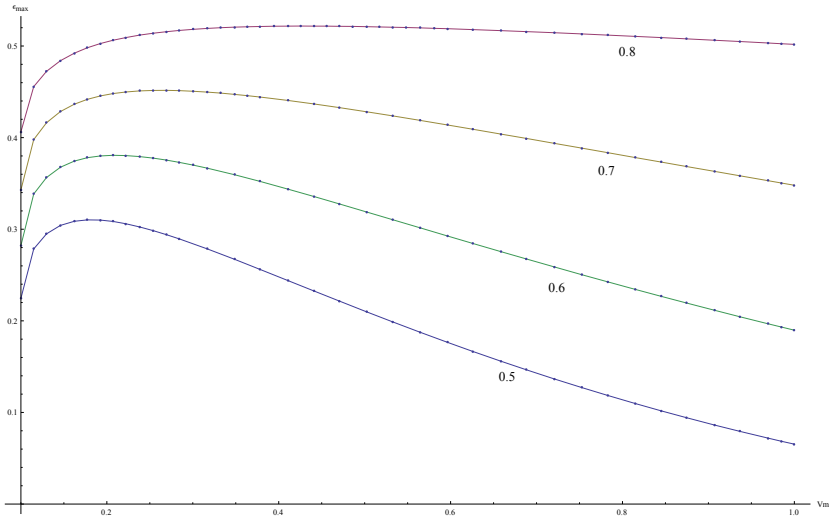

Figure 32: Dependency of maximal tolerable excess noise on side-channel input noise for squeezed state protocol for various coupling ratios S, $V = 1000$, $\eta = -3$dB

Thus, we have shown that additional modulation introduced on the input of side-channel can improve QKD protocols robustness to channel noise, and such modulation must be optimized in the given conditions.

6 Conclusions

We have investigated the influence of side channel loss on the security of the quantum key distribution schemes based on the coherent and squeezed state protocol upon realistic conditions of channel loss and channel excess noise. While the presence of side channel was shown not to be destructive for the secure key transmission, side channel still limits the robustness of protocols to noise in the quantum channel. It is shown that the key rates for both coherent and squeezed state protocols response to side channel information leakage in the same way, however squeezed-state protocol is more robust to it. We investigate the possibility to compensate the influence of side channel by inputting known and trusted noise into it. For both coherent and squeezed state protocols an optimal side-channel input noise can be found. Optimal input noise maximally decreases the negative effect on security of side channel. Moreover, such noise can increase the robustness of protocol to noise in the quantum (untrusted) channel. Further noise optimization should be considered. The investigation of additional realistic conditions can result in more effective optimization and may be the subject for further research.

References

[1] J. S. Bell. On the Einstein Podolsky Rosen paradox. In *Physics 1, Long Island City, N.Y.*, pages 195–200, 1964.

[2] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28:pp.656–715, 1949.

[3] T. Jennewein et al. A fast and compact quantum random number generator. *Rev. Sci. Instrum.*, 71:1675–1680, 2000.

[4] Shamir A. Rivest, R. L. and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21:120–126, 1978.

[5] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Symposium on Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society),Los Alamitos, California*, 1994.

[6] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, (IEEE, New York)*, pages 175–179, 1984.

[7] N. Herbert. Flash-a superluminal communicator based upon a new kind of quantum measurement. *Found. Phys.*, 12:1171–1179, 1982.

[8] W.K. Wootters and W.H. Zurek. Single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[9] D. Dieks. Communication by EPR devices. *Phys. Lett.*, 92A:271–272, 1982.

[10] W. Tittel N. Gisin, G. Ribordy and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 71:145–195, 2002.

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

[12] S. Popescu C. H. Bennett, H. J. Bernstein and B. Schumacher. Can quantum mechanical description of physical reality be considered complete? *Phys. Rev. A*, 53:2046, 1996.

[13] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[14] M.Hillery. Quantum cryptography with squeezed states. *Phys. Rev.*, A 61:022309, 1991.

[15] M. Levy N. J. Cerf and G. Van Assche. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, 2001.

[16] Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev.*, 88:057902, 2002.

[17] Vedral V., editor. *Modern Foundations of Quantum Optics*. Imperial College Press, 2005.

[18] Gerald J. Milburn D.F. Walls, editor. *Quantum Optics*. Springer, 2nd edition, 2005.

[19] Raul Garcia-Patron Sanchez. Quantum Information with Optical Continuous variables: from Bell tests to key distribution. Ph.D. thesis, UL Brussels, 2007.

[20] Gilles van Assche, editor. *Quantum cryptography and secret-key distillation*. University Press, Cambridge, 2006.

[21] F. Grosshans and P. Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. Internet: arXiv: quant-ph/0204127).

[22] J. Wenger et al. F. Grosshans, G. Van Assche. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421:238–241, 2003.

[23] W. P. Bowen T. Symul T. C. Ralph C. Weedbrook, A. M. Lance and P. K. Lam. Quantum cryptography without switching. *Phys. Rev. Lett.*, 93:170504, 2004.

[24] H. P. Yuen J. H. Shapiro and J. A. Machado Mata. Optical communication with 2-photon coherent states .3. quantum measurements realizable with photo-emissive detectors. *IEEE Trans. Inf. Theory*, IT-25:179, 1979.

[25] H. P. Yuen J. H. Shapiro. Generation and detection of two-photon coherent states in degenerate four-wave mixing. *Opt. Lett.*, 4:334–336, 1979.

[26] H. P. Yuen J. H. Shapiro. Optical communication with 2-photon coherent states .3. quantum measurements realizable with photo-emissive detectors. *IEEE Trans. Inf. Theory*, IT-26:78, 1980.

[27] H.Paul U. Leonhardt. Measuring the quantum state of light. *Progress in Quantum Electronics*, 19:89–130, 1995.

[28] S. L. Braustein. *Phys. Rev.*, A 42:474, 1990.

[29] W. Vogel and J. Grabow. *Phys. Rev.*, A 47:4427, 1993.

[30] Isaac L. Chuang Michael A. Nielsen, editor. *Quantum Computation and Quantum Information*. University Press, Cambridge, 2000.

[31] J. Wenger R. Tualle-Brouri F. Grosshans, N. J. Cerf and P. Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Inf. Comput.*, 3:535, 2003.

[32] G. Giedke M. M. Wolf and J. I. Cirac. Extremality of gaussian quantum states. *Phys. Rev. Lett.*, 96:080502, 2006.

[33] S. Chaturvedi R. Simon and V. Srinivassan. Congruences and canonical forms for a positive matrix: Application to the schweinler-wigner extremum principle. *J. Math. Phys.*, 40:3632, 1999.

[34] R.Garcia-Patron and N.J.Cerf. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.*, 102:120501, 2009.

[35] R. Filip. Security of coherent-state key distribution through an amplifying channel. *Phys. Rev.*, A 77:022310, 2008.

[36] R. Filip C. Usenko. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev.*, A 81:022318, 2010.

[37] S. Lloyd T.C. Ralph C. Weedbrook, S. Pirandola. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.*, 105:110501, 2010.

[38] S.Parameswaran J. Ambrose, A.Ignjatovic, editor. *Power Analysis Side Channel Attacks*. VDM Publishing, 2010.