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:	Optics and optoelectronics
Form of study:	Full-time
Supervisor:	Usenko Vladyslav, Dr.
Deadline:	25.07.2013

“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. As 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	53
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	53
Počet příloh	0
Jazyk	Anglický

Contents

1 Quantum Key Distribution protocols

1.1 Quantum key distribution

Cryptography has always been an important part of communication. The security of transmitted messages is very important today and throughout the history. With the advent of Internet, electronic business and online transactions that came later, cryptographic security became an integral part of modern life. Well-developed cryptographic protocols assure us that our personal information will remain secure during any online transactions. The ultimate dream of codemakers is to create such a protocol that will be impossible to crack and will remain secure and unbreakable in any circumstances and for any possible future technologies. Surprisingly, this protocol, the so-called One-Time Pad (OTP) was already invented and if used correctly this protocol cannot be cracked. OTP was proposed in years 1917-1926 by Gilbert Vernam [1]. It's predecessor, Vernam cipher, used similar coding system, but was vulnerable because secret key was reused after some time. OTP as many other cryptographic systems is based on the secret keys that should be available only to trusted parties, while the encrypted text can be publicly known.

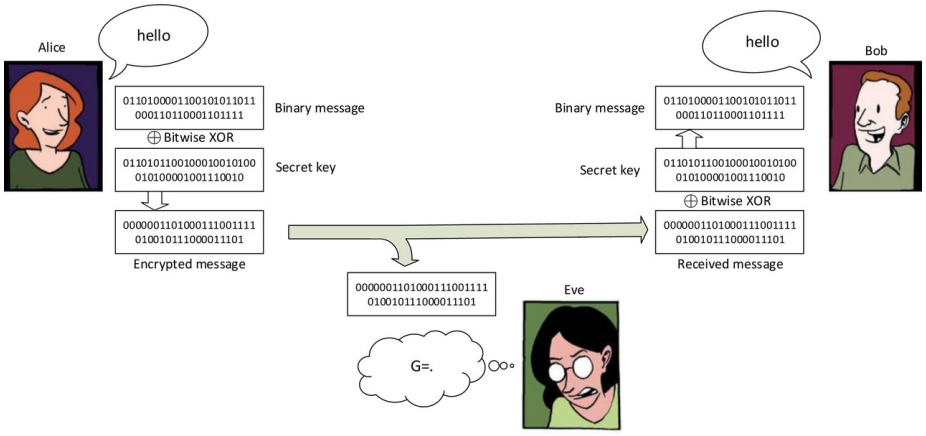

Figure 1: Illustration of one-time pad. Alice encodes her message using secure key by performing bitwise XOR operation. The encrypted message is sent to Bob through untrusted channel. Bob uses the same secure key and performs bitwise XOR operation on ciphertext to get the original message. Although Eve can copy the encrypted message she would not be able to decode it without secure key.

As illustrated on figure 1 OTP is an encryption algorithm that allows to encode text in ASCII using the secure key. This secure key has 3 requirements:

1. Key must have the same length as an original message.
2. Key must be random.

3. Key must be known only to trusted parties of communication.

Granted that the secure key will be used only once, the absolute security was proven by Claude Shannon [2].

Despite the proven security OTP suffers from practical implementation difficulties. These difficulties arise from previously stated requirements to the secure key. First of all, truly random numbers are difficult to obtain. Truly random numbers cannot be acquired from chaotic, but in principle classical processes, due to deterministic nature of classical physics. However truly random numbers can be generated with the use of elementary quantum processes [3]. Secondly, there is no way to fully securely distribute a key though untrusted channel. If there was a way to do this directly than protocols dealing with secure key transmission would not be needed. The main problems is that any kind of information encoded by classical means can be copied and duplicated. These limitations explain why OTP that theoretically provides impeccable security was used so rarely in practice. There are other protocols that use much shorter keys for secure communication, but these protocols are not as secure as the OTP.

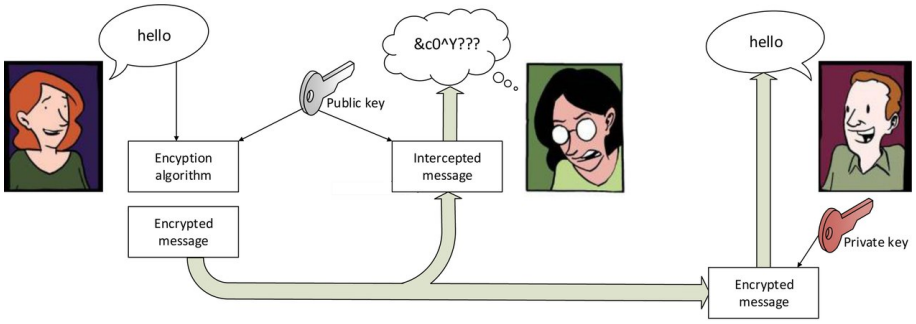

Figure 2: RSA protocol

Nowadays one of the most popular cryptographic scheme is RSA, named after its inventors - Ron Rivest, Adi Shamir and Leonard Adleman [4]. RSA is an asymmetric algorithm with a public key, based on computational complexity of finding prime factor of a large integer. In this scheme Bob prepares two different cryptographic keys - public key and private key. Public key can be acquired by anyone, but private key is known only to Bob. Alice can easily get a public key, use it to encode her message and send it to Bob via public channel. Eve, an eavesdropper, if she is listening to this public channel, can copy the encoded information but she will also need a copy of the private key, that can decrypt encoded message and is only known to Bob.

RSA algorithm, that belongs to public key cryptographic algorithms group, overcome the necessity of having trusted channel or trusted couriers, that deliver key to trusted parties through untrusted channel. This significant property of

RSA made it very popular amongst other cryptographic algorithms and widely adopted in modern cryptographic systems. Sadly, RSA is based on unproven mathematical assumption that there is no efficient way to find the prime factors of a large integer. Yet, this assumptions has not been proved and it's probable proof is still an open question. If an efficient way will be ever developed it would compromise most public cryptographic systems. Furthermore, an efficient factoring algorithm running on a quantum computer exists [5]. Possible connection of a quantum computer to modern networks will result in disastrous consequences. Although the creation of quantum computer is still a distant perspective, such a security threat cannot be disregarded.

Nevertheless the way to distribute secret keys through untrusted channels was found and is called quantum key distribution (QKD). QKD can be applied to other cryptographic schemes including previously mentioned OTP. QKD is based not on computational complexity but rather on limitations imposed by laws of physics.

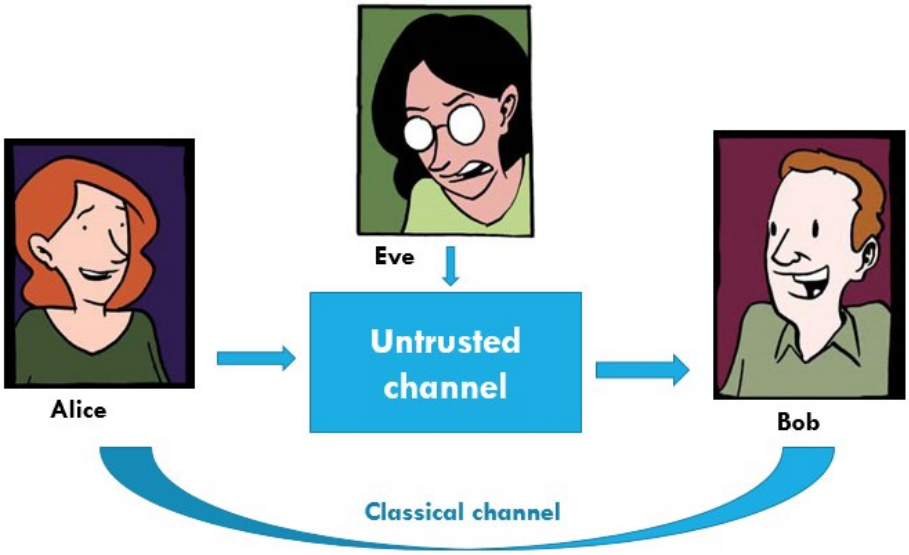

Figure 3: Quantum key distribution scheme

Presented on figure 3 is a general scheme of QKD that includes 3 main participants: Alice "the sender", Bob "the receiver" and powerful Eve "the eavesdropper". First of all, one makes an assumption that Eve possesses unlimited computational capabilities and is limited by laws of physics only. Secondly, Alice and Bob share two channels - authenticated classical channel and quantum channel (by quantum channel we mean a channel where quantum-information carriers propagate). Despite the fact that these main participants and their roles stay the same there are lots of possible types of QKD based on various information carriers, types of reconciliation, light sources etc.

QKD begins with the distribution of single quanta between Alice and Bob. Eavesdropping, from physical point of view, is an act of measurement or duplicating a distributed carriers of information, performed by an outside (untrusted) party. According to the rules of quantum mechanics, in general, any performed measurement inevitably modifies the state of the quantum particle. Any attempt of measurements in the untrusted transmission channel can later be discovered by Alice and Bob in a following public communication.

Any QKD based scheme, in general, proceeds as follows: Alice on her side prepares the information carrier, encodes information into it and then sends it to Bob through untrusted quantum channel (air, optical fiber). Initially we assume that Eve can fully control the quantum channel. After the information carrier got on Bob's side and was measured, Alice and Bob use authenticated classical channel for reconciliation. Both of them do not reveal information about detection results, so even if Eve is eavesdropping this classical channel she would not acquire additional information about the key.

1.2 The priciples of quantum cryptography

1.2.1 No-cloning theorem

The no-cloning theorem is one of the most earliest and important result in the study of quantum information. In 1982 N. Herbert proposed *FLASH*, a superluminal communication device based on quantum entanglement and on perfect cloning of an arbitrary unknown quantum state [6]. Herbert's suggestion conflicted with special relativity and aroused a huge debate in scientific community. Soon a refutations of his proposal, containing independently discovered quantum no-cloning theorem, were made by W.K. Wooters and W.H. Zurek [7] and D.Dieks [8].

No-cloning theorem is an important result of quantum mechanics and is utmost crucial for quantum key distribution. No-cloning theorem asserts that creation of identical copies of an arbitrary unknown quantum state is forbidden. If it was not, the cloning machine could be used to produce several identical copies of an unknown state, measurements on these copies could provide an information about conjugate properties of the state with high precision that violates uncertainty principle. No-cloning theorem is a consequence of linearity of quantum mechanics.

W.K. Wooters and W.H. Zurek provided a simple and intuitive proof [7]. Assuming that perfect cloning is possible a device that can create such replicas, the cloning machine, would have the following effect on an incoming qubit:

$$|A_0\rangle\,|\psi\rangle \rightarrow |A_\psi\rangle\,|\psi\psi\rangle \tag{1}$$

Here $|A_0\rangle$ is the initial state of the machine that is independent on the state of the incoming qubit, and $|A_\psi\rangle$is machine's final state, which may or may not depend on the state of original qubit that is intended to be cloned. Suppose that we want to clone a photon with certain polarization state. Than cloner will work for vertical polarizations as

$$|A_0\rangle\,|\updownarrow\rangle \rightarrow |A_{vert}\rangle\,|\updownarrow\updownarrow\rangle \tag{2}$$

and for horizontal polarizations

$$|A_0\rangle\,|\leftrightarrow\rangle \rightarrow |A_{hor}\rangle\,|\leftrightarrow\leftrightarrow\rangle \tag{3}$$

Such transformations should be represented by a linear operator. If initial photon is, for example, linearly polarized in $45\,^\circ$ direction, than its state can be written as $\alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle$, where $\alpha = \beta = \frac{1}{\sqrt{2}}$. Using equations (2) and (3) interaction of such a photon with cloning machine can be written as

$$|A_0\rangle\,(\alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle) \rightarrow \alpha\,|A_{vert}\rangle\,|\updownarrow\updownarrow\rangle + \beta\,|A_{hor}\rangle\,|\leftrightarrow\leftrightarrow\rangle \tag{4}$$

Generally cloning machine's states $|A_{vert}\rangle$ and $|A_{hor}\rangle$ after cloning procedure can be dissimilar, then photons at the output of the apparatus will be in a maximally mixed state. If apparatus states are identical than the output photons will be in a pure state.

$$\alpha\,|\updownarrow\updownarrow\rangle + \beta\,|\leftrightarrow\leftrightarrow\rangle \tag{5}$$

In neither of these cases output of the cloning machine contains two photons having $\alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle$ polarization. Therefore no device can perfectly clone an arbitrary polarization unless we have a prior knowledge that possible states of initial qubit are orthogonal.

Apparently no-cloning theorem imposes lots of limitations, but it turns out that they can be turned to advantages, and the biggest one is that this theorem allows us to reveal any communication eavesdropper since his presence inevitably disturbs the quantum state.

Quantum key distribution 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

BB84 is a QKD scheme developed by Charles H. Bennet and Gilles Brassard in 1984 [9]. and was a basis for the first quantum cryptography protocol. The protocol itself is secure due to previously described no-cloning theorem, it also is based on one-time pad encryption. Generally BB84 can be used for any kind of qubit - electron, photon etc.

Polarization qubits are commonly used in BB84, and we will use them for further description of the protocol. As previously mentioned 3 main participants take part in QKD. Alice wishes to send a private key to Bob, she uses 4 polarization states to encode bits of information: horizontal (H), vertical (V), diagonal (D, $45\,^\circ$) and anti-diagonal (A, $-45\,^\circ$). She can assign bit values of "0" and "1" to these respective polarization states, but commonly H or D represent "0" and V or A represent "1". Bob on his side has a detector that can measure

either in H and V basis (+)or in A and D basis (×). For each sent photon Alice randomly chooses a basis of polarization, as well as Bob randomly chooses the basis of the analyzer. If Bob's and Alice's basis were the same than Bob's measurement result will provide correct bit value with certainty. On the other hand if Bob will choose "wrong" basis, he will obtain a random result.

After receiving the incoming encoded message Bob uses authenticated classical channel to reveal to Alice the sequence of analyzers that he was using to detect photons. Alice tells him which times he used proper analyzer, but does not reveal the bit value. Next they conduct a reconciliation - process in which they discard all measurements for which Bob used the wrong analyzer, so that Alice and Bob at the end in principle will share the same bit sequence without any errors.

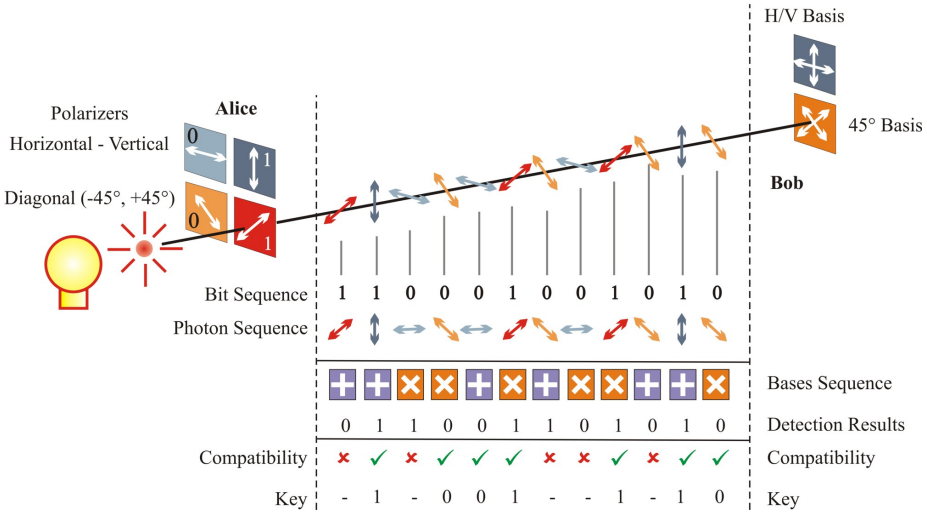

Figure 4: BB84 protocol. Alice encodes bit sequence onto photon polarization states and sends them to Bob, who chooses measurement bases, detects photons an obtains another bit sequence. Alice and Bob use classical channel to check whether Bob used a proper basis for every individual measurement therefore they sift second bit sequence and obtain secure key [10].

Eve, in her turn, must also guess which analyzer to use for measuring each photon sent by Alice. Despite any technological advancement that Eve can potentially posses, she still has a probability of $1/2$ to guess the correct analyzer. If she picks a correct analyzer, she can prepare and resend photon to Bob, but Eve will inevitably choose the wrong analyzer and will change the quantum state of the photon by her measurements. Consequently, when Bob receives a photon, he will occasionally get the wrong bit value even though he and Alice used the same polarization bases. Alice and Bob can take a small sample of their bit sequence and examine it for errors, that will allow them to determine

if an eavesdropper was present.

So after reconciliation Alice and Bob share the "sifted" bit sequence, that still may contain errors due to technical imperfections or Eve's intervention. Usually such errors are at rates of few percents. Conclusively, Alice and Bob should perform error correction, using any suitable error correction algorithm. Another important step - privacy amplification, that is done to reduce Eve's knowledge about the key. Both error correction and privacy amplification use part of the shared bit sequence and ultimately reduce the total length of it. For example during one of the plain error correction algorithms Alice chooses 2 bits from the shared bit sequence and discloses their XOR value. If Bob has the same XOR value for respective bits than he and Alice keep the first bit and discard the second bit from the chosen pair, if Bob's XOR value does not correspond to Alice's one than both of them discard both bits. There are a lot of other more complex and efficient error correction algorithms, but all of them inevitably reduce the key length. The same is true for privacy amplification. Here is the example of one of the possible algorithms. Alice chooses 2 bits from the sequence and calculate their XOR value, but this time she does not send the XOR value but the number of bits she has chosen (e.g. number 11 and 218). After this Alice and Bob replace these bits with their XOR value. This technique effectively reduces Eve's knowledge about the key, since she possess only partial information about the bits and she will have even less for their XOR value. If Eve knows the value of the first bit, but doesn't know anything about the second bit, than she cannot get their XOR value. For example 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 should be repeated numerous times, and can involve larger bit blocks for higher efficiency [11].

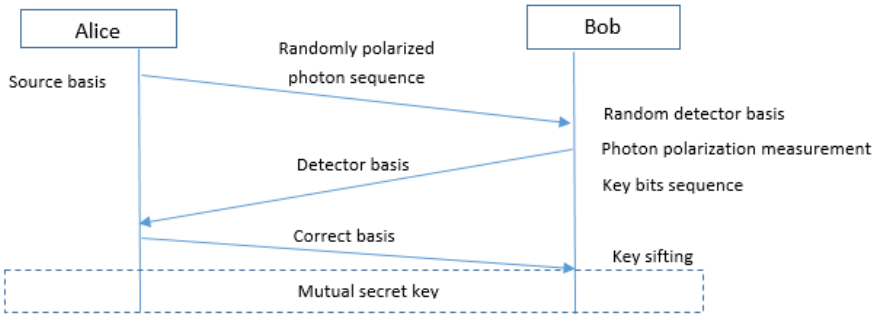

Figure 5: Information exchange between authenticated QKD parties

1.2.3 Entanglement based QKD

Quantum entanglement is an extremely interesting and peculiar phenomena in quantum mechanics. Firstly mentioned in well-known paper by Einstein,

Podolsky and Rosen in 1935 [12], entanglement has rapidly become one of the most perplexing and peculiar element of quantum mechanics mechanics. Quantum entanglement occurs when a pair of particles (photons, electrons, molecules etc.) 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. [13]. Generally speaking entanglement occurs when two physical systems interact and some correlation of quantum nature is generated between them. This correlation persists even when interaction stops and two systems are spatially separated[1] .

Quantum entanglement can be viewed as a form of quantum superposition. If one of the systems is measured separately, despite the location of the second system, measurement will cause the first system to take a definite value forcing the other entangled system to take respective correlated value. Entanglement is non-local and non-classical phenomena that can be described and comprehended only by means of quantum mechanics.

One can describe an arbitrary polarization state of a single photon 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, α and β are complex numbers that should satisfy the normalization condition $\alpha\alpha^* + \beta\beta^* = 1$. In this 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.

Entanglement of photons can be successfully used in QKD. Alice on her side can have an EPR source[2] and due to the main property of entanglement she

[1] Entanglement can be also created without direct interaction between the subsystems, via the so-called entanglement swapping [14].

[2] EPR source - light source that radiates a pair of entangled photons

can encode the information not by directly preparing the photon states but by measuring one of the photons therefore changing the other entangled photon. If Alice will conduct measurement in + basis she will detect H or V polarized photon with equal probability. Her measurement conditionally prepare the photon sent to Bob in the corresponding polarization state. If Bob subsequently measures his photon in the same basis, his result will be perfectly correlated to Alice's result. However, if Bob will conduct measurement in $\times$ basis, correlation will be absent. The final result will be the same if Bob will perform measurement before Alice or if both of them will use $\times$ basis.

The described above situation can be implemented in BB84 protocol as follows: EPR source is placed between Alice and Bob, one photon form the entangled pair is sent to each trusted party. For each incoming photon Alice and Bob randomly and independently choose measurement bases (+ or $\times$). After the transmission of the whole bit sequence, Alice and Bob using classical authenticated channel disclose the basis orientations that they were using for each photon but not the measurement result itself.

The main advantage of using EPR-source scheme is that Eve will gain no actual information by measuring transmitted photons, since there is no encoded information in them. The information is being encoded by the act of measurement itself, so it is much harder for Eve to obtain the key.

The first protocol using EPR source and advantages of entanglement was proposed by Artur Ekert in 1991 and is called E91 [15]. Since Eve intervention destroys the correlations between Alice and Bob, Ekert suggested to use Bell inequalities [16] for verifying the entanglement.

1.2.4 Continuous-variable protocols

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

The first continuous-variable protocol was developed by Hillery in 2000 [17]. He suggested a scheme that was using a squeezed light for information encoding. Squeezed light saturates uncertainty relation but quadratures noise is unequal. The character from an alphabet can be encoded into the value of quadrature that is being "squeezed". Scheme suggested by Hillery was very noise sensitive and required a high squeezing that can be challenging from technical point of view. Despite these disadvantages his idea became very popular due to numerous advantages. Unlike discrete-variable protocols the alphabet of continuous-variable protocols can be much bigger than "0" and "1".

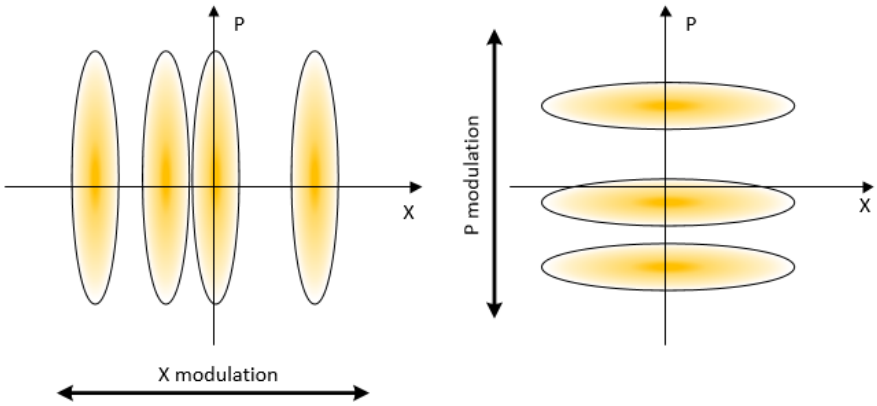

Figure 6: Squeezed state modulation in phase space x- quadrature (left) and p-quadrature (right)

Later in 2001, protocol was improved by Cerf [18]. 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 [19]. Using coherent states also allows to encode information in both quadratures. In other protocol suggested by Silberhorn et. al. [19] protocol, similarly to E91, Alice does not prepare a state but uses an EPR source and key is generated randomly during measurement processes. Despite relatively more complicated theoretical background of continuous-variable protocols comparing to discrete-variable ones, the first ones have a number of advantages:

- 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 used 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 compared 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.

1.3 Basics of continuous-variable protocols

1.3.1 Introduction to continuous-variable systems

A continuous-variable system is an infinite dimensional quantum system composed of N modes in a Hilbert space [13]

$$\mathscr{H} = \bigotimes_{k=1}^{N} \mathscr{H}_k \tag{6}$$

resulting from a tensor product of N infinitely-dimensional Fock spaces $\mathscr{H}_k$. These N modes can be seen as harmonic oscillators represented by following Hamiltonian

$$\hat{\mathcal{H}} = \sum_{k=1}^{N} \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right) \tag{7}$$

while each mode has different frequencies (ω_k), polarization or other properties. In equation (7) $\hat{a}^\dagger$ and $\hat{a}$ are creation and annihilation operators respectively. A creation operator increases the amount of particles in a respective state by one, and it is the adjoint of the annihilation operator and they both satisfy bosonic commutation relation:

$$\left[\hat{a}_k, \hat{a}_l^\dagger\right] = \delta_{kl}, \ [\hat{a}_k, \hat{a}_l] = \left[\hat{a}_k^\dagger, \hat{a}_l^\dagger\right] = 0 \tag{8}$$

The Fock space $\mathscr{H}_k$ is spanned by Fock basis $|n\rangle_i$ of eigenstates of the number operator $\hat{n} = \hat{a}^\dagger \hat{a}$. The vacuum state of the global Hilbert 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 (7).

For each mode corresponding quadrature operators can be defined as

$$\hat{x} = \hat{a}^\dagger + \hat{a}, \tag{9}$$

$$\hat{p} = i\,(\hat{a}^\dagger - \hat{a}). \tag{10}$$

The quadrature operators can be grouped in a vector

$$\hat{r} = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \ldots, \hat{x}_N, \hat{p}_N)^T \tag{11}$$

that also satisfies quadratures canonical commutation relation

$$[\hat{r}_i, \hat{r}_j] = i\Omega_{ij} \tag{12}$$

where Ω is the symplectic form

$$\Omega = \bigoplus_{i=1}^{N} \omega, \ \ \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{13}$$

In single-mode Hilbert space $\mathscr{H}_k$, the eigenstates of $\hat{a}_k$constitute the important set of coherent states [20]. 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

$$\hat{D}_k(\alpha) = \mathrm{e}^{\alpha\hat{a}_k^\dagger - \alpha^*\hat{a}_k} \tag{14}$$

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

1.4 Phase-space picture

It is convenient to treat quantum states of continuous-variable systems using not density operators ($\hat{\rho}$) on Hilbert space but functions defined on phase space. The complete description of quantum state can be provided by its characteristic function, which is related to Wigner function via Fourier transform. The Wigner function is quasi-probability function that connects wavefunction from Schrödinger's equation with phase-space. Using previously mentioned Weyl displacement operator, one can define the characteristic function as

$$\chi_\rho(\xi) = \mathrm{Tr}\left[\rho D_\xi\right], \tag{15}$$

where $\xi \in \mathbb{R}^{2\mathrm{N}}$ - vector on a real $2N$-dimensional space, which is called phase space. An arbitrary state can be written using equation (15) as

$$\rho = \frac{1}{(2\pi)^N} \int d^{2N}\xi \chi_\rho(-\xi) D_\xi. \tag{16}$$

The quasi-probability Wigner function can be written as

$$W(\xi) = \frac{1}{(2\pi)^N} \int d^{2N}\varsigma \mathrm{e}^{i\xi^T \Omega \varsigma} \chi_\rho(\varsigma). \tag{17}$$

There is an important set of Gaussian states that are characterized by Wigner functions, that are also Gaussian

$$W(\xi) = \frac{1}{\pi^{2N}\sqrt{\det\gamma}} \mathrm{e}^{-(\xi-D)^T\gamma^{-1}(\xi-D)} \tag{18}$$

here, γ is a symmetric covariance 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.

$$\gamma = \begin{pmatrix} \gamma_1 & \sigma_{1,2} & \cdots & \sigma_{1,n} \\ \sigma_{1,2}^T & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \sigma_{n-1,n} \\ \sigma_{1,n}^T & \cdots & \sigma_{n-1,n}^T & \gamma_n \end{pmatrix} \tag{19}$$

where diagonal elements γ_n consist 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.

Gaussian states are specific quantum states that found their usage in a great variety of quantum applications. Vacuum, coherent, thermal and squeezed states are all Gaussian states that are of utmost importance in quantum information and QKD. Covariance matrices (19) are necessary for description of Gaussian states and for further calculations in quantum information processing . It is important to mention that not every covariance matrix describes a real physical state. Covariance matrix describes a physical state if and only if $\gamma + i\Omega \geq 0$, Gaussian state is pure if and only if $\det \gamma = 1$ [20]. This condition is also necessary, although not sufficient for other non-Gaussian states.

The usage of covariance matrices greatly simplifies lots of calculations since they can be connected to all properties of quantum state. 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.

1.4.1 Vacuum, Coherent and Thermal states

The vacuum state is the state with the lowest possible energy. Generally it contains no physical particles. Usually vacuum is seen as an absolute emptiness and absence of any kind of energy, however it is not truly so. Vacuum contains fleeting electromagnetic waves and transient fluctuations that can exhibit many characteristics of an ordinary particle, but that exists for a limited time. Even though in quantum vacuum the average values of the fields vanish, their variances do not. Using phase space representation vacuum state can be described as the one that is located at the center of the phase space, in other words, vacuum state is a coherent state without displacement ($D = (0, 0)$). Minimal uncertainty is also characteristic property of vacuum state, therefore its covariance matrix is identity matrix ($\gamma = \mathbb{I}$).

Similarly to previous vacuum state definition, coherent state can be defined as a displaced vacuum state. Coherent state possess minimal uncertainty but contrary to vacuum state has a non-zero displacement.

$$|\alpha\rangle \equiv D(\alpha)\,|0\rangle \equiv \mathrm{e}^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}\,|0\rangle \tag{20}$$

Coherent state can be defined in other way: 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.

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{21}$$

Coherent states are closest states to classical theory, they can be reasonably well described from classical point of view, however full description can be made only using quantum mechanics. However one should not consider coherent state as classical state but rather as a quantum state that mimics some classical properties. [21].

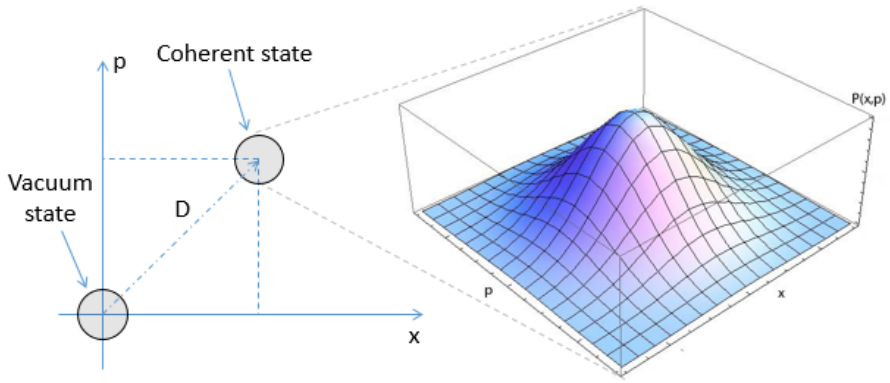

Figure 7: Vacuum and coherent states on phase space.

Thermal states have null mean value, but do not have minimum uncertainty and covariance matrix for an arbitrary thermal state can be written as

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

where quantity V shows the energy of the state and can be expressed through the number of photons n contained in the state as $V = 2n+1$. Vacuum state can be also viewed as a thermal state that has no photons at all ($n = 0$). Thermal state can be seen as a noisy version of coherent state.

1.4.2 Squeezed state

Previously described states have the same uncertainty in both quadratures, it means that the probability of detecting the encoded value is identical in both quadratures. In other words even though we displace the state on phase space

on the precise value due to fundamental uncertainty measurement will not give us the precise displacement value. One can consider this fundamental limitation as inevitable noise in quadratures.

Squeezed states have asymmetrical uncertainties in quadratures, one component has smaller than minimum uncertainty however the other component has uncertainty much bigger than minimum. Speaking in terms of fundamental detection noise - squeezed state's noise in one of the quadratures is lower than shot noise level, but simultaneously has increased fluctuations in other quadrature.

Squeezed state can be obtained by squeezing and displacing the vacuum state or vice versa by displacing the vacuum state therefore obtaining coherent state and squeezing it after. If minimum uncertainty relation holds than the degree of attenuation and amplification of respective quadratures is determined by squeezing factor r. The squeezed vacuum state has null mean value, but cannot be considered a vacuum state anymore since squeezed vacuum has significantly more energy than just a vacuum state. Covariance matrix for squeezed state is

$$\gamma = \begin{bmatrix} \mathrm{e}^{-2r} & 0 \\ 0 & \mathrm{e}^{2r} \end{bmatrix}, \tag{22}$$

where one can observe the squeezing in x- (if $r > 0$) or p- quadrature (if $r < 0$) and anti-squeezing in the conjugate one. Squeezed coherent state have similar covariance matrix but a non null displacement.

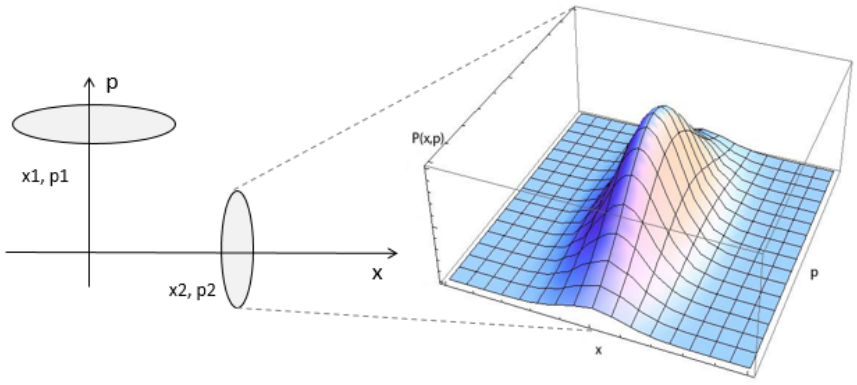

Figure 8: Squeezed states on phase space

1.5 Continuous-Variable Quantum Key Distribution

Discrete modulation of states is an integral part of discrete-variable protocols and obtaining a key as a sequence of ones and zeros is pretty straightforward but in case of continuous-variable various alphabets and modulations can be done that can lead to more efficient encoding and higher key rates [22].

1.5.1 A protocol with squeezed states

Squeezed state protocols are based on modulation of squeezed in one quadrature x (or p)-states. Displacement of these states gives, as an averaged result, a thermal state with a variance V. Firstly Alice picks a random variable a from Gaussian distribution (that is centered at zero and has a variance V_A) and displaces the squeezed vacuum state by its value ($d(0;0)\rightarrow(a,0)$ or $d(0;0)\rightarrow(0,a)$ depending on which type of squeezed state she will use). Provided that Alice will use x-squeezed states with a covariance matrix (22), averaging over all possible realizations will give us the mixed Gaussian state with null mean value and covariance matrix

$$\gamma_s = \begin{bmatrix} \mathrm{e}^{-2r} + V_A & 0 \\ 0 & \mathrm{e}^{2r} \end{bmatrix} \tag{23}$$

One can notice that $e^{-2r} + V_A = e^{2r}$ gives us a thermal state of variance $V = e^{2r}$. This state is indistinguishable from the thermal state that we would have ended up with if we used p-squeezed states and the same Gaussian distribution (centered at zero with variance V_A)

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

Such encoding gives us an advantage since in both cases the output mixed states have variance V and therefore equivalent.

Similarly to BB84 and other protocol communication procedure is a process that repeats for each light pulse: Alice generates a random number from a Gaussian distribution $V_A = e^{2r}$ (r - squeezing factor), than she randomly chooses what type of squeezed states to use x- or p- squeezed states and therefore applies proper displacement - $d_x = (a, 0)$ or $d_p = (0, a)$ respectively, where a - value of a previously generated number from Gaussian distribution (squeezing factor must satisfy $V_A = 2\sinh 2r$). In his turn, Bob also randomly selects which quadrature of the incoming pulse to measure x or p. After Bob successfully received and measured pulses sequence, he and Alice proceed with post-processing. First step is to "sift" a key: Alice uses classical authenticated channel to disclose the information to Bob whether she was using d_x or d_p, but not revealing the actual values. Consequently Bob keeps only the cases when he measured correct quadrature. Finally Alice and Bob use reconciliation protocols that are the combinations of error corrections and discretization and privacy amplification after [22].

Reconciliation, depending on what party is sending the information through classical channel, can be divided into:

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.

The production of squeezed states is quite challenging and difficult, contrary to them coherent states are more accessible and relatively easier to generate and manipulate. However if coherent states are considered as noisy versions of squeezed states, or squeezed states with small squeezing and used in previously described protocol the key rate will go to zero [18]. Solution was found in 2002 by Grosshans and Grangier, they suggested to modulate the prepared coherent states in both quadratures at the same time, this protocol was called GG02 [19]. This protocol reaches high secret-key rates [23] and performs relatively faster than BB84 due to the advantages and speed of homodyne detection comparing to photon detectors used in latter.

1.5.2 A protocol with coherent states

In the standard GG02 protocol, Alice encodes two different key elements, one of which will be discarded by Bob. The thermal state with variance V can be still obtained by bi-variate Gaussian mixture of coherent states. Alice picks random variable (a_x, a_p) from the bi-variate Gaussian distribution (as before centered at zero with variance V_A) encodes it the coherent state by respectively displacing it $d_{xp} = (a_x, a_p)$. Therefore turning covariance matrix for coherent state

$$\gamma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

into

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

By setting a proper V_A ($V_A = V - 1$) and averaging over all possible realizations, one can obtain a thermal state with variance V [20].

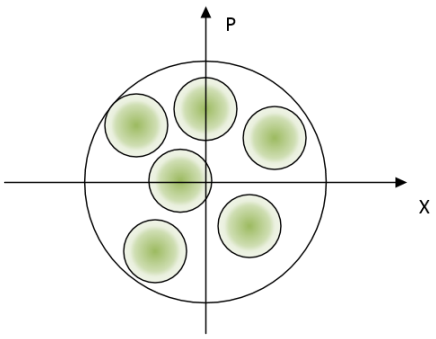

Figure 9: Alice can generate coherent states with mean value (a_x, a_p) according to a Gaussian distribution (variance V_A). The mixture is equivalent to a thermal state ($V = V_A - 1$).

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 the same step for each sent pulse: firstly Alice generates two random numbers a_x and a_p from two independent Gaussian distributions but with the same variance V_A. Alice displaces the state by $d_{xp} = (a_x, a_p)$ and sends it to Bob via untrusted quantum channel. Bob, in his turn, randomly chooses which quadrature to measure x or p. After Bob successfully received and measured pulses sequence, he and Alice proceed with post-processing. Bob using classical authenticated channel discloses the information about which one of the quadratures he was measuring for each pulse, but does not reveal anything about the measurement results. Alice keeps the measured by Bob value and discards the other quadrature. After the sifting they proceed with discritezation, error correction and privacy amplification.

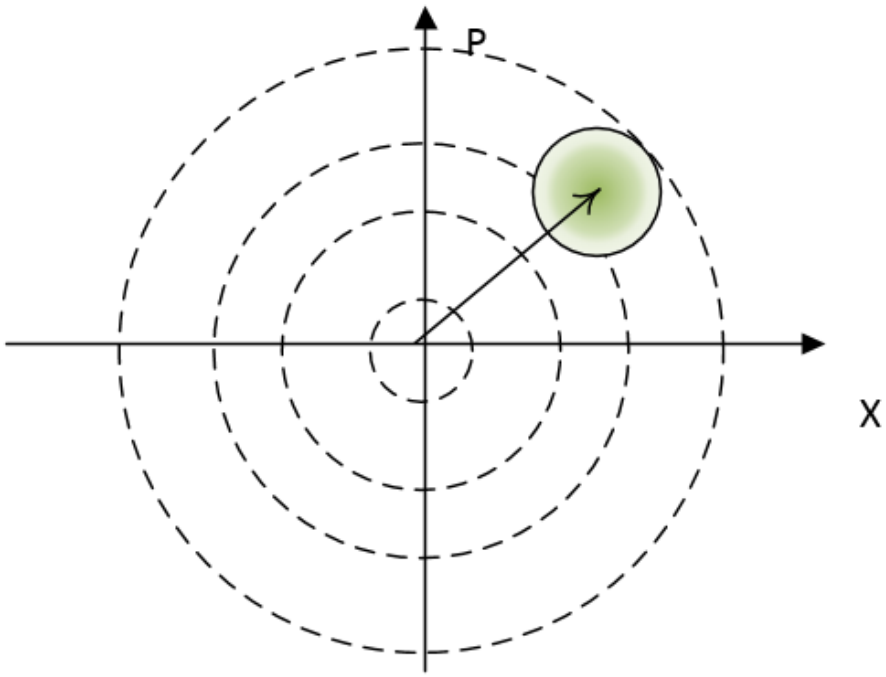

Figure 10: Schematic description of the encoding. The coherent states, such as the one illustrated in the upper right quadrant, are modulated along both axes. Their centers follow a bivariate Gaussian distribution, illustrated by the concentric circles.

Considering that Alice uses two numbers and two quadratures to encode the information and Bob uses only one of them, this allows to reach high secret-key rates since the "*useful*" information is contained in each sent pulse. However, one

can modify the coherent state protocol [19] in order to use both values [24]. The suggestion is to use heterodyne detection instead of homodyne. In heterodyne detection balanced beamsplitter is used to divide the incoming pulse into two and to measure x-quadrature and p-quadrature separately and simultaneously. This protocol is called *no basis switching protocol*.

1.6 Homodyne detection

Homodyne detection is an extremely powerful and useful tool in QKD. Such kind of detection allows us to measure phase sensitive properties of the impinging light fields and therefore acquire information about quantum states of light. The crucial part of homodyne detection is a reference radiation - local oscillator, that is usually a light beam in a coherent state with large photon number or non-modulated part of the incoming signal beam. Produced by signal and local oscillator beams interference fringes vary with different phase between the two fields that allows us to observe quantum statistics of the signal and subsequently acquire the information about the quantum state of the signal [25].

Lets describe the properties of the most common tool - balanced homodyne detector. Balanced homodyne detector consists of 50:50 beam splitter, two photodetectors and electronic circuit [26].

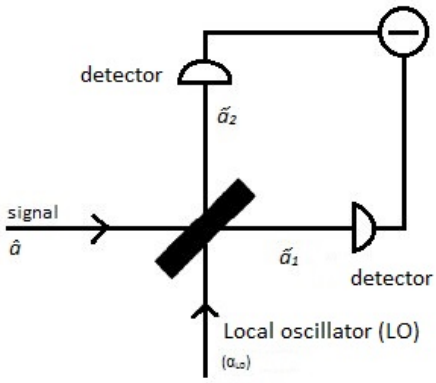

Figure 11: Balanced homodyne detector. The signal is optically mixed with a strong coherent local oscillator using a 50:50 beam splitter. The emerging fields are detected and the photocurrents are electronically subtracted to yield the measured quantity.

The signal and local oscillator beam are mixed on a beam splitter. Photodetectors are detecting the outputs of the beamsplitter, measure photocurrent and

subsequently subtract measured values:

$$\triangle \hat{J} = \hat{a'}_2^{\dagger}\hat{a'}_2 - \hat{a'}_1^{\dagger}\hat{a'}_1 = \frac{1}{2}\left(\hat{a}^{\dagger} + \hat{a}_{LO}^{\dagger}\right)(\hat{a} + \hat{a}_{LO}) - \frac{1}{2}\left(\hat{a}^{\dagger} - \hat{a}_{LO}^{\dagger}\right)(\hat{a} - \hat{a}_{LO}) = \\ = \hat{a}^{\dagger}\hat{a}_{LO} + \hat{a}\hat{a}_{LO}^{\dagger}. \quad (24)$$

Provided that local oscillator beam is coherent and intense (has large photon number), comparing to original signal field, it can be described classically by substituting the annihilation operator $\hat{a}_{LO}$ with complex amplitude $\alpha_{LO} = |\alpha_{LO}|\,\mathrm{e}^{i\theta}$. In this case photocurrent difference is rewritten as

$$\triangle \hat{J} = |\alpha_{LO}|\left(\hat{a}\mathrm{e}^{-i\theta} + \hat{a}^{\dagger}\mathrm{e}^{i\theta}\right). \quad (25)$$

Equation equation (25) is not applicable for all cases, but remains correct for local oscillator's highly excited coherent state. Thus balanced homodyne detector directly measures quadratures of the quantum state of light

$$\triangle \hat{J} = |\alpha_{LO}|\sqrt{2}\cdot\hat{x}_{\theta} \quad (26)$$

namely a combination of quadratures corresponding to a rotation $\hat{x}(\Theta) = \hat{x}\cos\Theta + \hat{p}\sin\Theta$. The phase difference between the signal and local oscillator defines the rotation angle. Therefore changing the phase one can obtain needed information about the respective quadrature.

More complex and detailed description using quantum-statistical theory can be found in [26, 27, 28].

2 Entropy and information

2.1 Shannon entropy

The most crucial part of any information theory is a quantification of information. Entropy is a key concept of information theory. Entropy is a measure of uncertainty about the state of the physical system. Classical theory uses a conception of Shannon entropy. Shannon entropy quantifies on average how much information one can gain about some random variable X after sequence of measurements. It can also be defined as follows: the entropy of X measures the amount of uncertainty about X before one learns its value (measures it). These two definitions are complementary, entropy can be represented either as a measure of uncertainty before one learns the value of X, or as a measure of information gained after the measurement of X [29].

One of the important properties of entropy is that the type or content of random variable does not depend on the labels attached to different values this variable can take. For instance, if we have a system that can take values "+" or "-" with respective probabilities 1/5 and 4/5, the entropy for such system will be the same as for the one where variable takes values "0" and "1" with the same respective probabilities 1/5 and 4/5. Accordingly, the entropy should be defined in such a way that its value will be dependent only on probabilities values that

variable can take, and not by the labels that are attached to these values. The Shannon entropy defined in terms of probability distributions is

$$H(X) \equiv -\sum_x p_x \log_2 p_x. \tag{27}$$

The entropy can be measured in "bits", "nats" or "bans", the most suitable for our purposes is the usage of "bits" evaluation. The logarithm in equation (27) may cause some troubles in interpretation of entropy since $\log 0$ is undefined. Intuitively an event that does not occur should not contribute to the entropy, by convention for this case $0 \log 0 \equiv 0$, or more formally $\lim_{x \to 0} x \log x = 0$ [29].

There are lots of types of different entropies in information theory. One of them, the relative entropy is a measure of closeness of two probability distributions $p(x)$ and $q(x)$, over the same index set, x. For these distributions it can be defined by

$$H(p(x)|q(x)) \equiv \sum_x p(x) \log_2 \frac{p(x)}{q(x)} \equiv -H(X) - \sum_x p(x) \log_2 q(x). \tag{28}$$

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 can be used to express other types of entropies and as a interconnection between them.

While previous entropies are dealing with distribution of one random variable there are entropy extensions that deal with more than one random variable.One of them is the joint entropy. It is defined as

$$H(X,Y) = -\sum_{x,y} p(x,y) \log_2 p(x,y) \tag{29}$$

and expresses the total uncertainty about the pair of random variables X and Y.

The conditional entropy gives us an averaged value of how uncertain we are about the random variable X, provided that we know the value of Y.

$$H(X|Y) \equiv H(X,Y) - H(Y). \tag{30}$$

Another quantity the mutual information shows how much content does X and Y have in common. But suppose that we add the information about X, $H(X)$, to the information about Y, $H(Y)$. Shared between X and Y information, in this case, will be counted twice, while information unique to X and to Y will be counted only once. In order to get the mutual information, we need to subtract the joint information $H(X,Y)$ from this sum

$$H(X:Y) \equiv H(X) + H(Y) - H(X,Y) \tag{31}$$

in terms of conditional entropy mutual information can be written as

$$H(X:Y) = H(X) - H(X|Y). \tag{32}$$

All mentioned previously special cases of entropies can be deduced using depicted on Venn diagram. This diagram is not completely reliable for comprehension of properties of entropies, however it provides a clear understanding of relations between entropies and their properties.

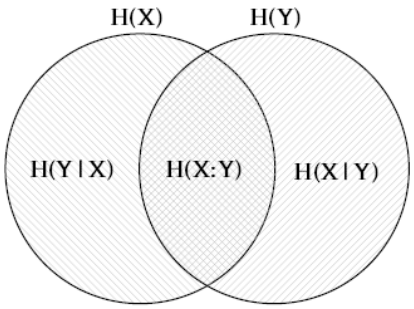

Figure 12: Relationships between different entropies.

Basic properties of Shannon entropy:

- $H(X,Y) = H(Y,X)$, $H(X:Y) = H(Y:X)$.
- $H(Y|X) \geq 0$ and thus $H(X:Y) \leq H(Y)$, with equality if and only if Y is a function of X, $Y = f(X)$.
- $H(X) \leq H(X,Y)$, with equality if and only if Y is a function of X
- $H(X,Y) \leq H(X) + H(Y)$ with equality if and only if X and Y are independent random variables.
- $H(Y|X) \leq H(Y)$and thus $H(X:Y) \geq 0$, with equality in each if and only if X and Y are independent random variables.
- $H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z)$, with equality if and only if $Z \to Y \to X$ forms a Markov chain.
- $H(X|Y,Z) \leq H(X|Y)$

2.2 Von Neumann entropy

The extension of the concept of entropy to quantum mechanics was presented in a famous book "Mathematische Grundlagen der Quantenmechanik" in 1932 by Johann von Neumann [30]. While the Shannon entropy deals with classical probability distributions, von Neumann entropy uses density operators.

The Von Neumann entropy is defined using quantum state ρ as

$$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho). \tag{33}$$

Equation (33) can also be expressed via eigenvalues λ_x of the state ρ

$$S(\rho) = -\sum_x \lambda_x \log_2 \lambda_x \tag{34}$$

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

Similarly to the Shannon entropy it is useful to define the relative entropy that can be used in quantum mechanics. Suppose ρ and σ are density operators. The relative entropy of ρ to σ is defined by

$$S(\rho||\sigma) = \mathrm{Tr}(\rho \log_2 \rho) - \mathrm{Tr}(\rho \log_2 \sigma). \tag{35}$$

The non-negativity of quantum relative entropy is described by Klein's inequality [31]:

The quantum relative entropy is non-negative ,

$$S(\rho||\sigma) \geq 0, \tag{36}$$

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

Basic properties of Von Neumann entropy:

- The entropy is non-negative. The entropy is zero if and only if the state is pure.
- 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 $\mathbb{I}/d$.
- Suppose a composite system AB is in pure state. Then $S(A) = S(B)$.
- Suppose p_i are probabilities, and the states ρ_i have support on orthogonal subspaces. Then

$$S\left(\sum_i p_i \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i). \tag{37}$$

- 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

$$S\left(\sum_i p_i |i\rangle\langle i| \otimes \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i). \tag{38}$$

2.3 Holevo bound

In quantum information theory there is a great need of knowing how much information can be contained in a quantum system, in other words - accessible information. Unfortunately, there is no general method for calculating this bound, however exists a great variety of proven important bounds and one of the most important of them is the Holevo bound [32].

Suppose that Alice prepares a set of mixed states $\{\rho_1, \rho_2, ..., \rho_n\}$. One of the states - ρ_x, where $X = 0, ..., n$, is drawn accordingly to the probability distribution $\{p_0, ..., p_n\}$. Bob performs a POVM on the state and acquire measurement result Y. The Holevo's theorem states that for any possible measurement Bob may achieve:

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x), \tag{39}$$

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

Thus the Holevo bound is an upper bound on the accessible information. The right side of the (39) is called the Holevo information or Holevo χ quantity.

The accessible information does not commonly saturate Holevo bound. One can see that in order to saturate the Holevo bound using product measurements the states must have orthogonal support, which is not generally satisfied. Nonetheless collective measurements on the signal can achieve the Holevo bound and this is the main reason why this bound found such a wide usage in theory of QKD.

3 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 is mainly done using an entanglement-based scheme, as they are completely equivalent [33] but latter significantly simplifies calculations or makes them possible in principle.

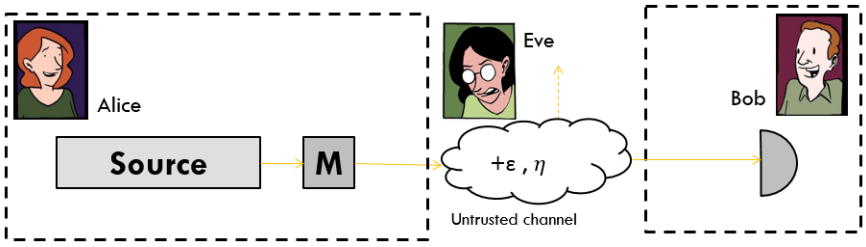

Figure 13: Prepare-and-measure protocol scheme

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 using methods described previously and then sends the states through untrusted quantum channel they states suffer from losses (η) and excess noise (ϵ) and finally arrive to Bob's side, where they are being detected and processed further.

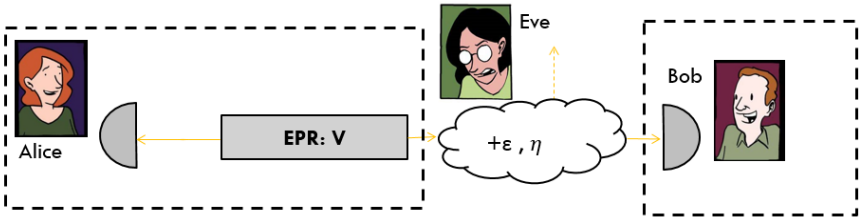

Figure 14: Entanglement-based protocol scheme with squeezed states. For coherent states heterodyne measurement on Alice's side should be used.

In entanglement-based scheme Alice on her side generates an entangled state using an EPR source, 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.

3.1 Individual attacks

Individual attacks are those in which Eve is restricted to interact with and measure each transmitted signal independently. It was proven [34] 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

$$\gamma_{AB} = \begin{bmatrix} \gamma_{AB}^{x} & 0 \\ 0 & \gamma_{AB}^{p} \end{bmatrix} \tag{40}$$

Security is shown as the positivity of the key, following Csiszar - Korner theorem [11], in other words the information transmission is secure until key rate reaches zero.

Key rates for direct reconciliation and reverse reconciliation are expressed through mutual information between participants of QKD and can be written respectively as:

$$K_{DR} = I_{AB} - I_{AE}, \tag{41}$$

$$K_{RR} = I_{AB} - I_{BE}, \tag{42}$$

where I is mutual information (equation (31)) between respective parties. Roughly speaking protocol remains secure until the information that Alice and Bob share is bigger than the information known to Eve. In terms of equation (32) key rates can be written as:

$$K_{DR} = H\left(A|E\right) - H\left(A|B\right), \tag{43}$$

$$K_{RR} = H\left(B|E\right) - H\left(B|A\right). \tag{44}$$

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

$$H\left(X|Y\right) = \frac{1}{2}\log_2 V_{X|Y}, \tag{45}$$

where entropy is measured in bits, so the final result would give us quantity of bits per pulse.

Mutual information written in conditional variances:

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}}, \tag{46}$$

and variances itself as:

$$V_{X|Y} = V_X - \frac{C_{XY}^2}{V_Y}, \tag{47}$$

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 that Eve holds the purification of state ρ_{AB}. Using previously described entropies and Heisenberg equation one can write:

$$V_{A|E}V_{A|B} \geq 1 \tag{48}$$

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 (48) can also be written in terms of measured quadratures for different types of reconciliations, but general meaning stays the same.

3.1.1 Pure losses

Let us first consider a purely lossy channel. During calculations it was assumed that all other devices in schemes are ideal, working with maximum possible efficiency and noise and transmission losses are introduced in the quantum channel. Expressions for mutual information between Alice and Bob, Alice and Eve and Bob and Eve can be respectively written as,

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

$$I_{ae} = \frac{1}{2}\log_2\left(\frac{V}{V - \frac{(1-\eta)(V^2-1)}{\eta+(1-\eta)(k+V)}}\right) \tag{50}$$

$$I_{be} = \frac{1}{2}\log_2\left(\frac{1-\eta+\eta(k+V)}{1-\eta+\eta(k+V) - \frac{\sqrt{\eta(1-\eta)}(1-k-V)^2}{\eta+(1-\eta)(k+V)}}\right) \tag{51}$$

Graph representations of equations (49,50,51) are shown on figure 15.

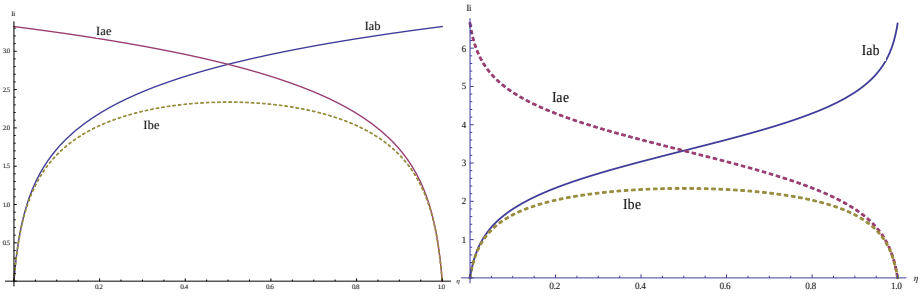

Figure 15: Dependencies of mutual information (left - coherent states protocol, right - squeezed state protocol) on channel losses,where I_{ab}, I_{ae}, I_{be}- mutual information between Alice and Bob, Alice and Eve, Bob and Eve respectively.

On figure 15 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. Noticeably mutual information between Alice and Bob increases with the decrease of losses, correspondingly mutual information between Alice and Eve decreases since Eve receives less information when data leakage in untrusted channel is smaller. However for any values of losses mutual information between Eve and Bob remains smaller than the one between Alice and Bob. One can conclude that direct reconciliation becomes insecure if $\eta < 0.5$, while reverse reconciliation can tolerate any pure loss.

3.1.2 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:

$$N = \frac{\eta\varepsilon}{1-\eta} + 1. \tag{52}$$

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:

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{\eta V(V+\epsilon-1)+V}{\eta+\eta V(\epsilon-1)+V}\right) \tag{53}$$

$$I_{AE} = \frac{1}{2}\log_2\left(\frac{V(\eta+\eta V(\epsilon-1)+V)}{\eta(V+\epsilon-1)+1}\right) \tag{54}$$

$$I_{BE} = \frac{1}{2}\log_2\left(\frac{(\eta+\eta V(\epsilon-1)+V)(\eta(V+\epsilon-1)+1)}{V}\right) \tag{55}$$

On figure 16 one can we can see a difference between the squeezed state and coherent state protocols, more specifically - coherent state protocol is less robust to noise.

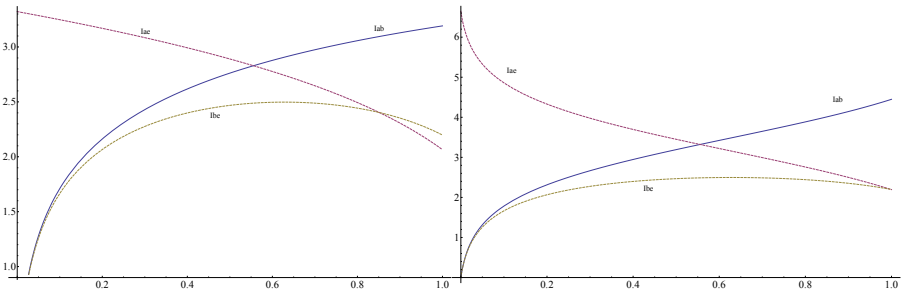

Figure 16: Mutual information on channel losses. Left - coherent state protocol, Right - squeezed state protocol, $\epsilon = 0.2$, $V = 100$

3.2 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 (39). 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:

$$K_{DR} = I_{AB} - \chi_{AE}, \tag{56}$$

$$K_{RR} = I_{AB} - \chi_{BE}. \tag{57}$$

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:

$$S_X = \sum_n G\left(\frac{\lambda_n - 1}{2}\right), \tag{58}$$

where

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x. \tag{59}$$

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

$$K_{DR(RR)} = I_{AB} - S_E + S_{E|A(E|B)} = I_{AB} - G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right), \quad (60)$$

where λ_n - symplectic eigenvalues of a respective covariance matrix.

Due to Williamson theorem [35] we know that for any N-mode covariance matrix γ there is a symplectic transformation S such that:

$$S\gamma S^T = \lambda \quad (61)$$

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

$$\lambda = \bigoplus_{k=1}^{N} \begin{bmatrix} \lambda_k & 0 \\ 0 & \lambda_k \end{bmatrix}. \quad (62)$$

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,

$$\mu = \mathrm{Tr}\rho^2 = \frac{1}{\sqrt{\det\gamma}}. \quad (63)$$

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

$$\det\gamma = \det\lambda = \prod_{i=1}^{N} \lambda_i^2. \quad (64)$$

The most basic 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:

$$\det\gamma_{AB} = \lambda_1^2\lambda_2^2. \quad (65)$$

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 number of modes situation is much complicated and generally cannot be solved and simplified analytically [20].

4 Advanced security

4.1 Preparation noise

In ideal case when there are no losses and noise, and detectors are ideal, the process of obtaining secure key between trusted parties is plain and straightforward. 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 [36]. On the other hand, trusted preparation noise can break the security of coherent-state protocol [37] already for the pure loss in the case of reverse reconciliation, but can be compensated with proper purification [38]. In our theoretical analysis we consider both coherent and squeezed state protocols.

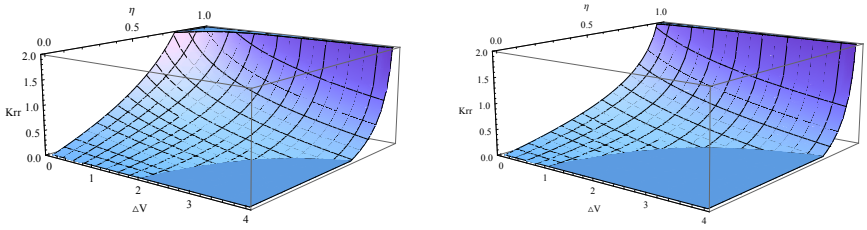

Figure 17: Dependency of key rate for reverse reconciliation on channel losses and preparation noise $\triangle V$ for squeezed (left) and coherent (right) state protocol.

One should emphasize that preparation noise, if it is on the reference side of reconciliation, does not break the security [20, 39].

First, we generalize the study of the preparation noise to the squeezed state protocol [11]. For purely lossy channels in case of infinitely squeezed states expression for preparation noise that breaks the security can be written as,

$$\triangle V = \frac{2-\eta}{1-\eta} \tag{66}$$

and for coherent state protocol with arbitrary large source variance [37] it is known as more strict bound:

$$\triangle V = \frac{1}{1-\eta} \tag{67}$$

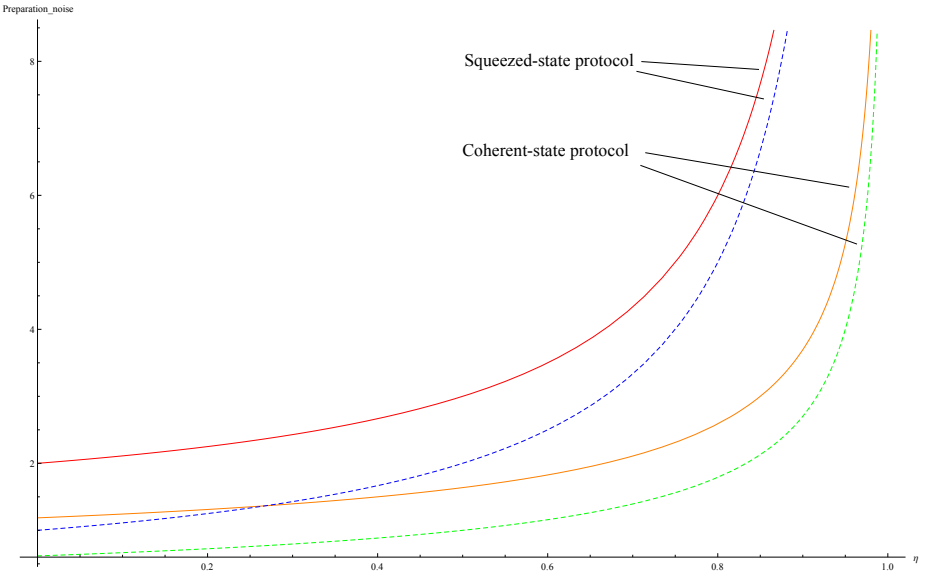

Figure 18: Comparison of dependencies of maximum tolerable preparation noise on channel losses between squeezed and coherent state protocols for purely lossy channel, for infinitely high variance $V \to \infty$ (solid) and mild variance $V = 2$ (dashed).

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

$$\triangle V = \frac{2 - \eta - \eta\epsilon^2 + 2\eta\epsilon - 2\epsilon}{1 - \eta + \eta\epsilon}. \tag{68}$$

As can be seen from figure 18 squeezed state protocol is more robust against the preparation noise upon the same energy of the signal states.

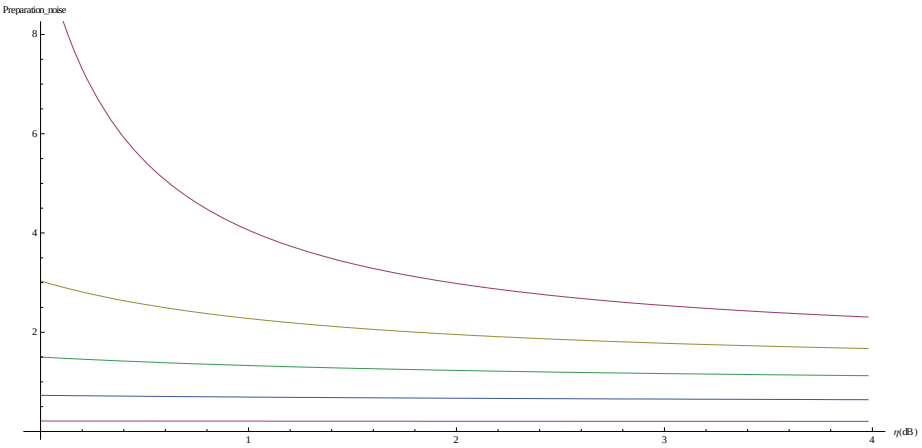

Figure 19: Dependency of maximum tolerable preparation noise on channel losses (in dB) for various influences of excess noise ε, where starting from top curve $\varepsilon = 0.1,\ 0.3,\ 0.5,\ 0.7,\ 0.9$

4.2 Side channel

It is reasonable to assume that attackers will try any means possible to break the security of information transmission. Computational complexity that lays in the basis of any protocol can be weakened or even bypassed using additional information, therefore it is necessary to investigate all possible ways attackers can "backdoor" the security. Attacks that are based on information obtained from physical implementation of a cryptosystem instead of exploiting theoretical weaknesses or cryptoanalysis are called side-channel attacks. Timing information, power consumption, electromagnetic fields, dissipating heat 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.

There are a few types of side channel attacks:

- Invasive and non-invasive: Invasive attacks require direct access to the inside components of the cryptographic device while non-invasive attacks only exploit externally reachable information.
- Active and passive: Active attacks try to alter in a specific way the functionality of the cryptographic device while passive attacks are entirely based on observations and do not disturb the working process of the device.

In further calculations we consider that Eve can carry non-invasive passive attack. Such kind of attacks do not require any sophisticated and expensive equipment and they pose a serious threat to any cryptographic system.

In classical cryptography there are lots of different classes of passive 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 [40]. Further we consider effect on side-channels in CV QKD.

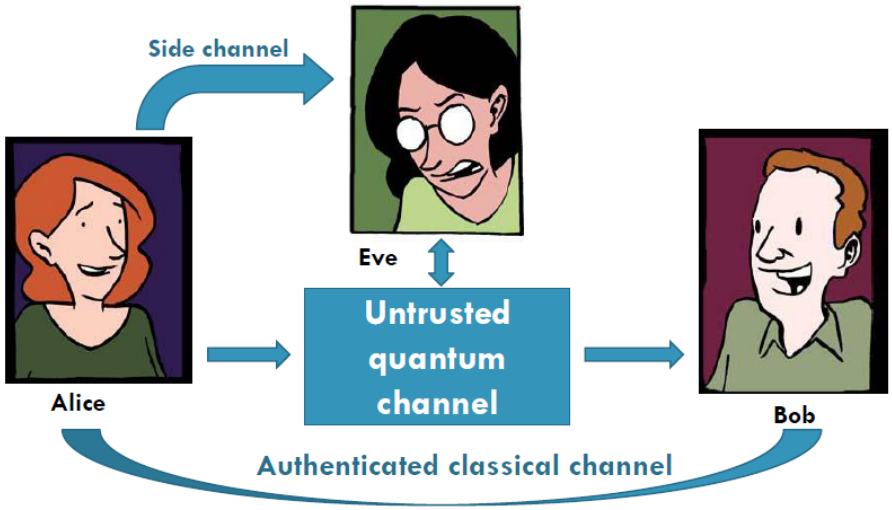

Figure 20: Side channel in QKD

Side channels are present in all QKD systems due to the imperfections of equipment. However 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.

4.2.1 Vacuum input

In QKD we introduce side channel to the system as an additional beamsplitter on trusted side. The reflectance of this beamsplitter is proportional to leakage of the main signal to the side channel.

Let us consider the side-channel loss, where the input of a side-channel is a vacuum state coupled to a signal with ratio S and is not by any means controlled by Eve (figure 21,22). However Eve can use this side channel to gain knowledge about the key without introducing errors and therefore does not reveal herself. 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 (46) are

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}}\,, \tag{69}$$

$$I_{BE} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|E_1E_2}}\,, \tag{70}$$

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 (47)), 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

$$K_{(S)RR} = \frac{1}{2}\log_2 \frac{1}{(1-\eta S)^2} \tag{71}$$

$$K_{(C)RR} = \frac{1}{2}\log_2 \frac{1}{1-\eta S} \tag{72}$$

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

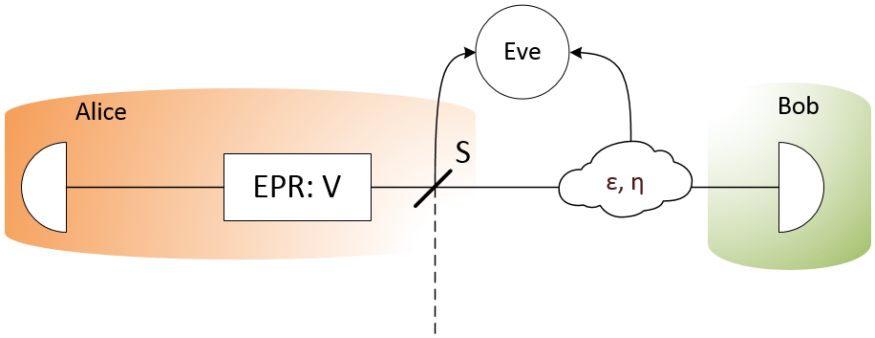

Figure 21: General EPR based quantum key distribution scheme with a side channel

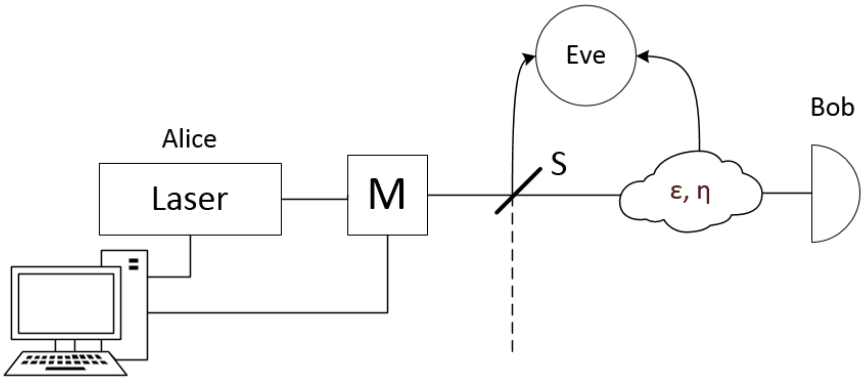

Figure 22: General Prepare & Measure based quantum key distribution scheme with a side channel

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 23 coherent state protocol is less robust to excess noise than squeezed state protocol.

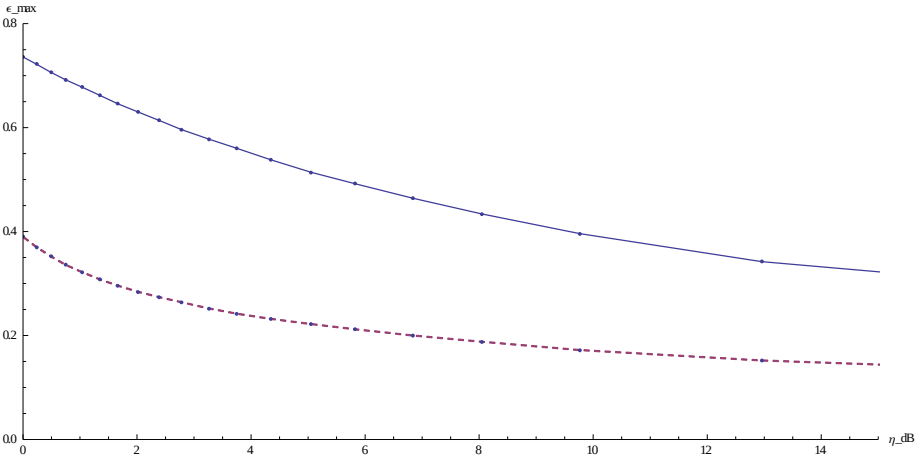

Figure 23: Comparison between coherent (dashed) and squeezed state protocols for maximum tolerable excess noise on channel losses (in dB) in absence of side-channel.

However side-channel decreases robustness of protocols to excess noise as seen from figure 24.

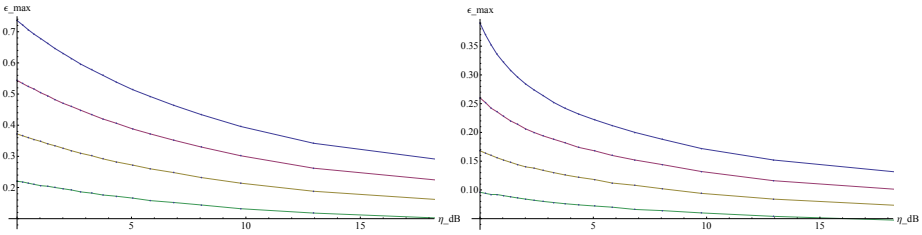

Figure 24: Side channel influence on squeezed (left) and coherent (right) state protocols for different coupling ratios (starting from top $S = 1,\ 0.8,\ 0.6,\ 0.4$, where 1 stands for absence of side-channel)

As can be seen from figure 24 when side channel coupling ratio to signal is small more informaion flows into side channel, tolerance to channel excess noise decreases and eventually reaches zero therefore protocol is no longer secure for any values of excess noise. However we are interested in values of coupling rations or in other words level of presence of side channel that are still tolerable for the security.

4.2.2 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 25, 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.

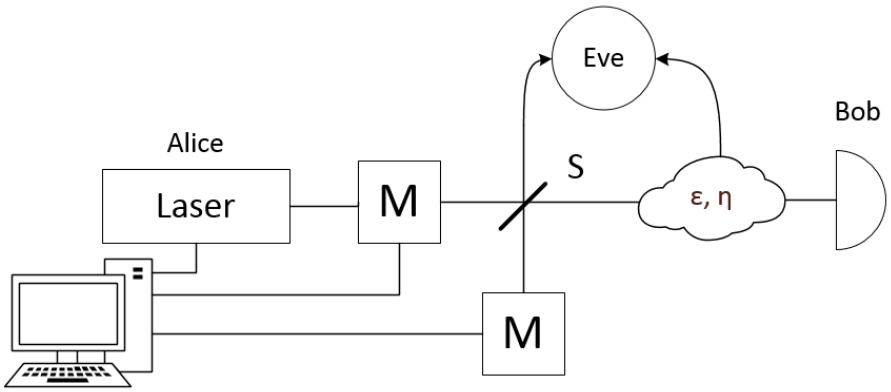

Figure 25: Prepare & Measure based side-channel quantum key distribution scheme with additional modulation input to side-channel

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 referred 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

$$K_{(S)RR} = \frac{1}{2}\log_2\left(\frac{\eta S}{\eta\left(V_m - 2\sqrt{-(S-1)S}V_m - S\right)+1}\right) - \frac{1}{2}\log_2\left(\frac{\eta S(1-\eta(S+V_m)+V_m)}{V_m+1}\right) \tag{73}$$

$$K_{(C)RR} = \frac{1}{2}\log_2\left(\frac{\eta S}{-2\eta\sqrt{-(S-1)S}V_m + \eta V_m + 1}\right) - \frac{1}{2}\log_2\left(-\frac{\eta S(\eta S + (\eta-1)V_m - 1)}{V_m+1}\right) \tag{74}$$

As was mentioned previously EPR scheme is completely equivalent to P&M scheme. Corresponding EPR scheme to P&M scheme on figure 25 is shown on figure 26.To purify modulation, 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 sent 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. First mode from EPR:N source is sent through beam-splitter with reflectance T into the side channel, another mode with reflectance $(1-T)$ is coupled to the Alice's signal mode. The reflectance for second beam-splitter should be very low, so main signal mode won't be altered too much, but Alice's detection should provide information on both modes.

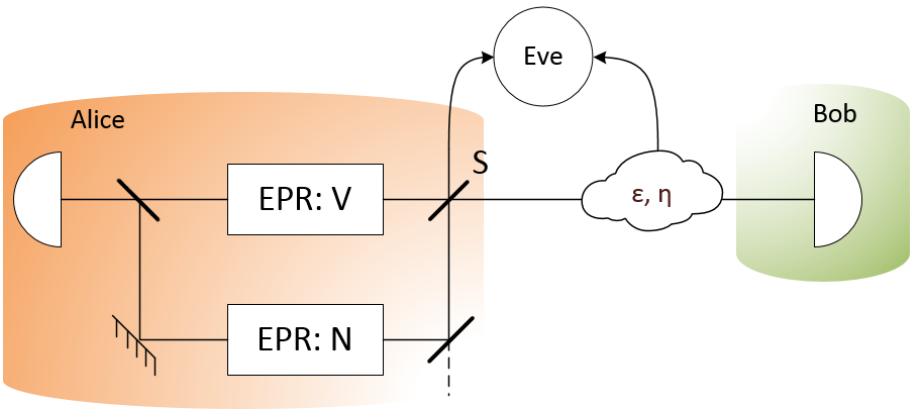

Figure 26: EPR based side-channel quantum key distribution scheme

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. The area below the dependency curve is the area of a positive key rate and secure protocol. As can be seen on figure 27 - 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 excess 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".

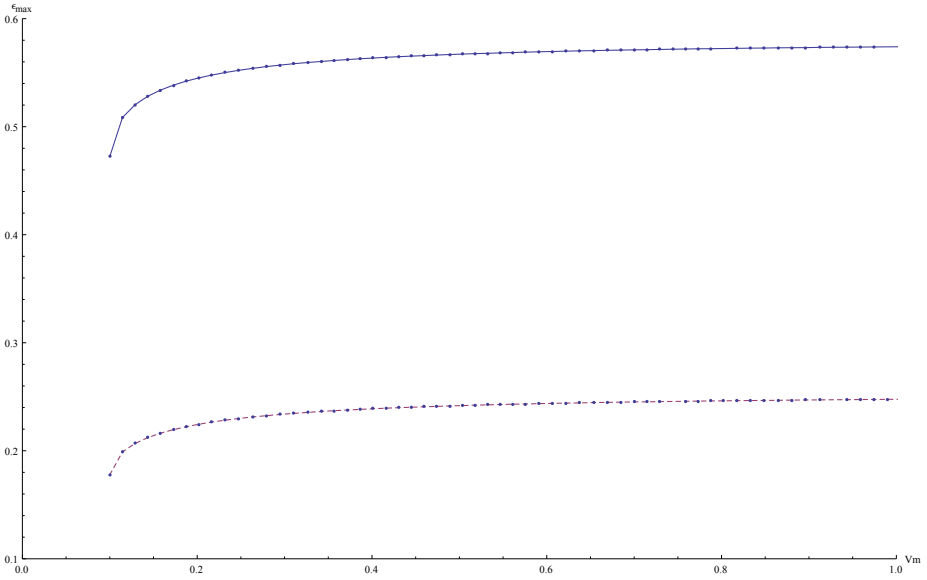

Figure 27: Dependency of maximal tolerable excess noise on side channel input noise for coherent (dashed) and squeezed state protocols. Side channel coupling ratio $S = 0.9$, $V = 1000$, $\eta = -3$dB.

Further calculations show that side-channel input noise can actually have positive impact on security of quantum key distribution. The behavior of dependency of key rate on side-channel input noise is similar to the dependency of maximum tolerable excess 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 interesting 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.

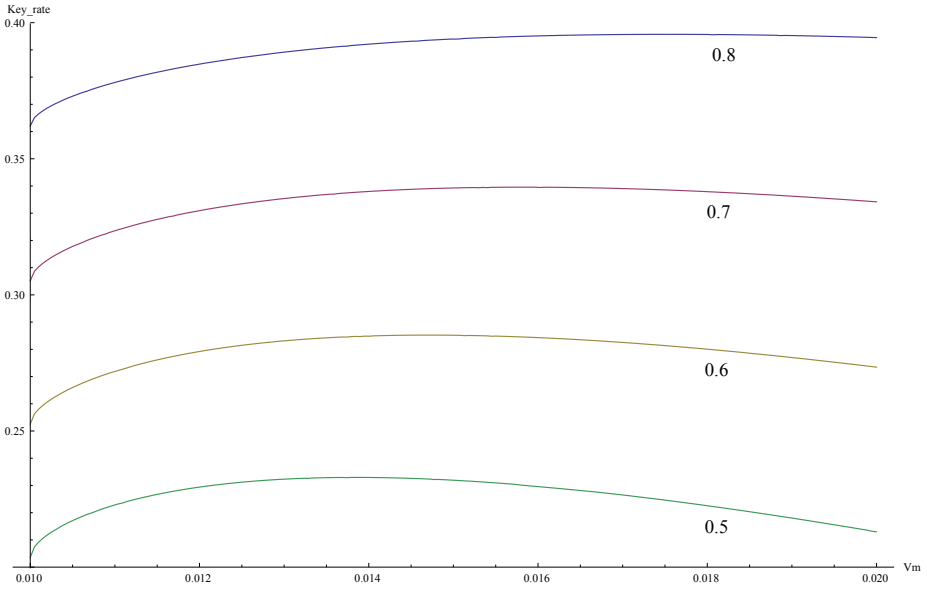

Figure 28: Coherent state protocol key rate depending on side-channel input noise for different side channel coupling ratios S. $V = 1000,\ \epsilon = 0,\ \eta = -3\text{dB}$

The same effect can be seen for squeezed state protocol.

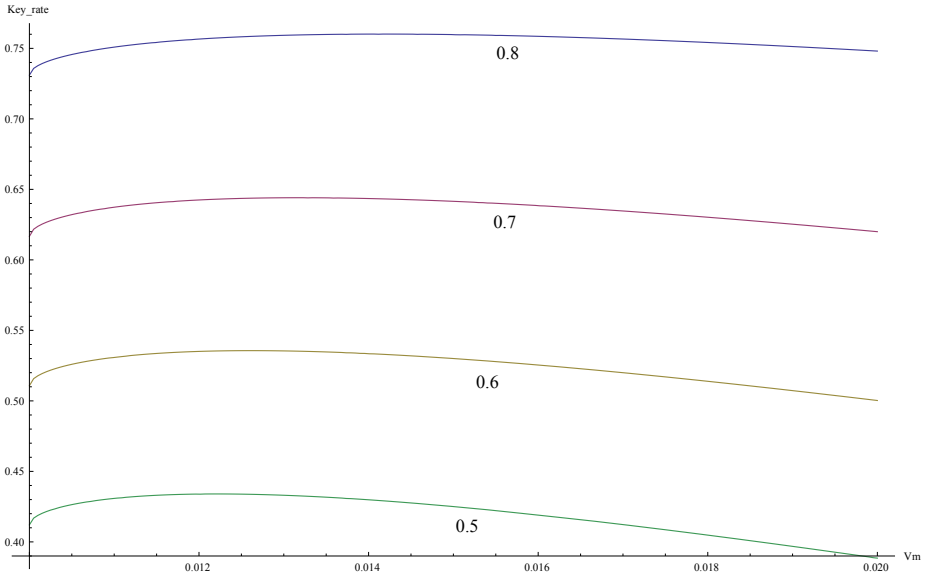

Figure 29: Squeezed state protocol key rate depending on side-channel input noise for different side channel coupling ratios S. $V = 1000,\ \epsilon = 0,\ \eta = -3\text{dB}$.

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

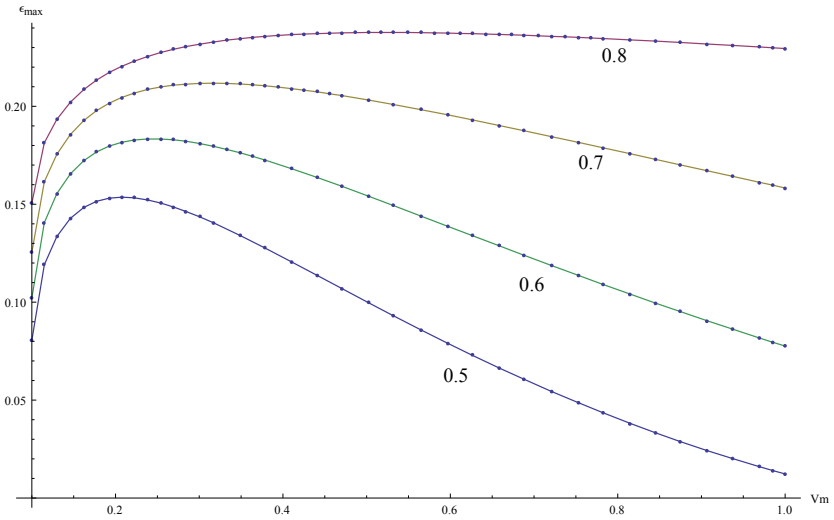

Figure 30: Dependency of maximal tolerable excess noise on side-channel input noise for coherent state protocol for various coupling ratios S, $V = 1000$, $\eta = -3$dB

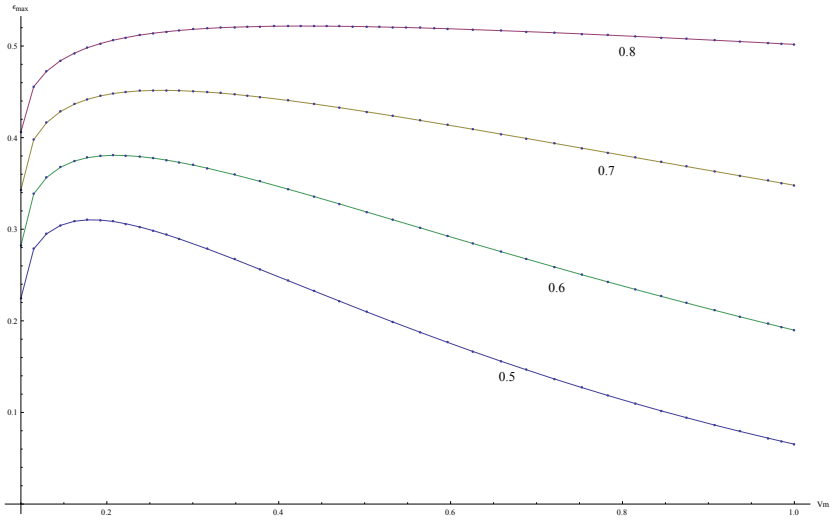

Figure 31: Dependency of maximal tolerable excess noise on side-channel input noise for squeezed state protocol for various coupling ratios S, $V = 1000$, $\eta = -3$dB

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.

5 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] G.S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. IEEE*, 55:109–115, 1926.

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

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

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

[9] 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.

[10] G. Weihs W. Tittel. Photonic entanglement for fundamental tests and quantum communication. *Quantum Inf. Process.*, 1:3, 2001.

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

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

[13] Gerardo Adesso. Entanglement of Gaussian States. Ph.D. Thesis, University of Salerno, 2007.

[14] 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.

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

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

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

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

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

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

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

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

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

[24] 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.

[25] Tomas Opatrny Dirk-Gunnar Welsch, Werner Vogel. Homodyne detection and quantum state reconstruction. *Progress in Optics*, XXXIX:63–211, 2009.

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

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

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

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

[30] J. von Neumann, editor. *Mathematische Grundlagen der Quantenmechanik.* Springer Verlag, 1932.

[31] O. Klein. Zur quantenmechanischen begrundung des zweiten hauptsatzes der warmelehre. *Z. Physik*, 72:767–775, 1931.

[32] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *[Probl. Inf. Transm.*, 9:110, 1973.

[33] 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.

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

[35] 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.

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

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

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

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

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