Performance Evaluation of Scalar Reconciliation for Continuous-Variable Quantum Key Distribution

Albert Mraz, Sandor Imre, Laszlo Gyongyosi
Department of Networked Systems and Services
Budapest University of Technology and Economics (BME)
H-1117 Budapest, Magyar tudosok krt. 2.
Email: {mraz, imre, gyongyosi}@hit.bme.hu

***Abstract*—The existing robust technique, Scalar Reconciliation combined with a Continuous-Variable Quantum Key Distribution is investigated in this paper with the help of simulations in terms of the symbol error rate. The solution contains efficient logical layer-based reconciliation for Continuous-Variable Quantum Key Distribution techniques, which extract the binary information from correlated Gaussian variables. The algorithm has been extended by different assumptions related to the raw data generation method and the segmentation of the key symbols to be transmitted. The performance of the extended algorithm has been investigated in terms of the symbol error ratio.**

Keywords: continuous-variable quantum key distribution, reconciliation, Gaussian variables, quantum cryptography, simulation, symbol error rate.

I. Introduction

The Quantum Key Distribution (QKD) solutions play key role in the world of practical applications of quantum information theory, allowing unconditionally secret communication by exploiting the fundamental attributes of quantum mechanics. The QKD protocols are classified into two main groups: Discrete-Variable (DV) and Continuous-Variable Quantum Key Distribution (CVQKD) systems. DV QKD protocols are based on discrete variables (photon polarization). In a CVQKD the information is encoded on continuous variables with the help of Gaussian modulation. In this case the modulation and decoding of continuous variables does not require specialized equipments and can be realized effectively in current communication systems.

We can divide the CVQKD protocols for two further types: one-way and two-way systems. In a *one-way* CVQKD system Alice (transmitter) sends the continuous variables to Bob (receiver) over a quantum channel [1], [2], [3]. In a *two-way* system, Bob starts to communicate, Alice receives the message and adds the secret information to that, the result is then sent back to Bob. The two-way CVQKD systems [4], [5], [6], [7] were introduced to solve the deficiencies of one-way CVQKD, such as low key rates and short communication distances. The CVQKD schemes apply continuous-variable Gaussian modulation, providing provably optimal key rates against collective attacks at finite-size block lengths, and also maximizing the mutual information between Alice and Bob.

A key part of the CVQKD is *post-processing*, which corrects the effects of the noise, appearing as errors in the raw data. Raw data is a correlated bitstring at Alice's and Bob's side, generated as a results of random quadrature measurements. Each measurement is represented as a unit in the raw data. The raw data contains no secret information. The secret key is a *uniformly distributed* binary string, which will be combined with the raw data elements. During the post-processing phase we use classical-authenticated communication channel and *classical* error-correction algorithms. The logical-layer based post-processing corresponds to the tomography in the physical layer, and it consists of the *reconciliation* procedure with error-correction steps, and *privacy amplification*. The theory of the logical layer-based reconciliation enables also to view the noise affected physical quantum channel as a binary Gaussian channel in the logical layer [1], [2], [3], resulting that classical well-known error correction techniques can be involved into CVQKD, which would not be available for the physical-layer tomography to extract the binary information from the correlated Gaussian variables.

The noisy raw data on the quantum channel shall be corrected in order to get the secret key. The amount of raw data bits is considerably large, hence the complexity of the post-processing phase should be as low as possible. The existing solutions need complex calculations for the reconciliation of Gaussian variables. The error correction in the reconciliation phase consists of two phases: First, the binary-channel codes (low-density parity-check (LDPC), turbo codes, polar codes, etc. [1], [2], [3]). Second, the correction of the erroneous received raw-data vector passed through the quantum channel.

The authors of [8] focused on the second phase, considering the reconciliation problem analogous to the binary-channel coding, they replaced the complicated physical-layer tomography in the logical level by simpler binary error-correction schemes. Current paper introduces additional assumptions for the distribution of the raw data, and gives different segmentation methods of the key information to be transmitted. Finally, the results of a simulation-investigations of the extended CVQKD solution are provided in [8].

This paper is organized as follows: Section II contains the block diagram and the variables of the algorithm's mathematical model defined in [8], in Section III we propose different random distributions for the raw data elements, Section IV describes the transmission of the key sequence on the classical channel and provides different methods for the segmentation of the information. In Section V the reception method on the

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

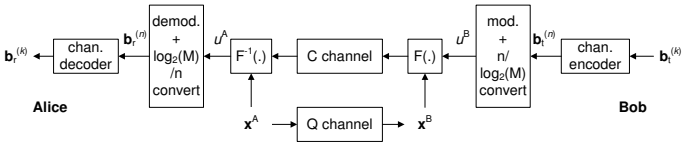

Fig. 1. Block scheme of the quantum key distribution

classical channel is described, followed by simulation results related to the different assumptions for the raw data generation and key segmentations.

II. System Model

In this section we provide a mathematical model for the Continuous-Variable Quantum Key Distribution solution introduced in [8] focusing on the exact definition of the variables. The block scheme of the key transmission can be observed at Fig. 1. During the operation Bob initiates the reconciliation process (upper arrows from right to left), after the quantum communication ends (lower arrows from left to right). This diagram illustrates a reconciliation process in a one-way CVQKD.

At the block scheme $u^{\mathrm{B}} \in \mathbb{R}$ refers to the secret key symbol of Bob to be transmitted towards Alice on the *classical channel*, which can be generated with the help of Amplitude Shift Keying (ASK), based on a pre-defined input bit sequence. During an observed transmission period a single u^{B} symbol will be transmitted. The received key-symbol will be denoted by $u^{\mathrm{A}} \in \mathbb{R}$. The vector

$$\mathbf{x}^{\mathrm{A}} = (x_1^{\mathrm{A}}, ..., x_i^{\mathrm{A}}, ..., x_d^{\mathrm{A}}) \in \mathbb{R}^d \tag{1}$$

contains d pieces of raw data elements at Alice's side. In addition

$$\mathbf{n} = (n_1, ..., n_i, ..., n_d) \in \mathbb{R}^d \tag{2}$$

represents d size noise vector at the quantum channel, containing independent and identically distributed (i.i.d.) Gaussian Random Variables (RVs) with 0 mean and $N_0^{(q)}$ variance.

The raw data of Bob is contained in the d sized vector

$$\mathbf{x}^{\mathrm{B}} = (x_1^{\mathrm{B}}, ..., x_i^{\mathrm{B}}, ..., x_d^{\mathrm{B}}) \in \mathbb{R}^d, \tag{3}$$

we define it according to

$$\mathbf{x}^{\mathrm{B}} = \mathbf{x}^{\mathrm{A}} + \mathbf{n}. \tag{4}$$

The k length bit sequence $\mathbf{b}_{\mathrm{t}}^{(k)}$ represents the input of the channel encoder, the n length $\mathbf{b}_{\mathrm{t}}^{(n)}$ bit sequence means the output of the channel encoder, both at Bob's side. At the side of Alice, the channel decoder has an n length input bit sequence $\mathbf{b}_{\mathrm{r}}^{(n)}$ and a $\mathbf{b}_{\mathrm{r}}^{(k)}$ output bit sequence with length of k.

The **mod.+**$n/\log_2(M)$ **convert** block contains an M level ASK modulator and a buffer. During its operation it stores the n length $\mathbf{b}_{\mathrm{t}}^{(n)}$ bit sequences, transforms them to bit sequences with length of $\log_2(M)$ and modulates them. Its output is the u^{B} key symbol.

The functional element **demod.+**$\log_2(M)/n$ **convert** involves an M-ASK demodulator and a buffer; it generates $\log_2(M)$ length bit sequences based on the u^{A} key symbols, stores them and transforms to n length $\mathbf{b}_{\mathrm{r}}^{(n)}$ bit sequences. The $\mathrm{F}^{-1}(.)$ and $\mathrm{F}(.)$ blocks will be introduced later in (16)).

"C channel" and "Q channel" are representing the classical- and quantum channels respectively.

III. Information on the quantum channel

The elements of the d length $\mathbf{x}^{\mathrm{A}} = (x_1^{\mathrm{A}}, ..., x_i^{\mathrm{A}}, ..., x_d^{\mathrm{A}}) \in \mathbb{R}^d$ vector, containing Alice's raw data will be generated according to the following different distributions:

A. Truncated Gaussian distribution

The raw data elements will be modeled as Gaussian RVs with 0 mean and $\sigma_{x_A}^2$ variance, which will be adjusted during the simulations based on the noise energy and the *desired* Signal-to-Noise-Ratio (SNR). The truncation happens according a to pre-defined $\sqrt{E_{X_{\mathrm{A}}}^{\max}}$ maximal signal level on the quantum channel, under that the transmission still have a 'quantum-behvaiour'. A discrete signal can be defined by the raw data elements, which has an energy of

$$E_{X_{\mathrm{A}}} = \sum_{i=1}^{N} \left| x_i^{\mathrm{A}} \right|^2, \tag{5}$$

considering N samples.

In case of the Gaussian raw data generation the energy amount above can be calculated as

$$E_{X_{\mathrm{A}}} \approx N\sigma_{x_A}^2, \tag{6}$$

as long as $\sqrt{E_{X_{\mathrm{A}}}^{\max}} >> \sigma_{x_A}^2$, i.e. in this case the interval of the truncation does not affect significantly the energy of the Gaussian raw data signal.

B. Uniform distribution

In this case the raw data elements will be generated according to uniform distribution with the interval of $\left[-\sqrt{E_{X_{\mathrm{A}}}^{\max}}, \sqrt{E_{X_{\mathrm{A}}}^{\max}}\right]$.

The energy of N samples of generated discrete signal x_i elements according to a continuous uniform distribution on the $[a, b]$ interval can be expressed as

$$\begin{aligned} E_x &= N\frac{1}{(b-a)}\int_a^b x^2 du = N\frac{1}{(b-a)}\left[\frac{x^3}{3}\right]_a^b \\ &= N\frac{b^3-a^3}{3(b-a)}, \end{aligned} \tag{7}$$

for $b > a$.

By substituting the interval of the raw data elements (i.e. $b = -a = \sqrt{E_{X_{\mathrm{A}}}^{\max}}$), we get the energy of N elements from the raw data at Alice's side, which can be calculated in this case as

$$E_{X_{\mathrm{A}}} = N\frac{E_{X_{\mathrm{A}}}^{\max}}{3}. \tag{8}$$

Note that the energy expressions above will be used to set a desired SNR value during the simulations (see eq. (18)).

IV. Information on the classical channel

This section contains the description of the transmission on the classical channel involving the modulation and different segmentation models of the u^{B} key symbols.

A. Modulation

During the modeling of the modulation process we generate the bit sequence $\mathbf{b}_{\mathrm{t}}^{(k)}$ according to discrete uniform distribution from the set 0 and 1, representing the input of the channel encoder.

The channel encoder will provide the $\mathbf{b}_{\mathrm{t}}^{(k)}$ bit sequence based on a selected encoding method. Using the $\mathbf{b}_{\mathrm{t}}^{(k)}$ bit sequence we generate u^{B} (real valued) key symbols with the help of an $M = 2^k$ level ASK modulator.

Note that the application of ASK can be explained by the real (i.e. not complex) property of u^{B}. That is Quadrature Amplitude Modulation (QAM) cannot be applied, since in that case we would get *complex* key symbols.

B. Segmentation of the key symbols

In the following, we transmit a *single* u^{B} symbol during a single transmission step over the *classical channel*, segmented into d elements. For this segmentation we define the following three different ways.

1) Uniform distribution, determining the last element: A segmentation is performed on symbol u^{B}, after which we get the sum of

$$u^{\mathrm{B}} = \sum_{i=1}^{d} u_i^{\mathrm{B}}. \tag{9}$$

Our goal in ideal case would be that the u_i^{B} elements are *uniform* RVs with the sum 'accidentally' equal to u^{B}.

Unfortunately this task cannot be performed practically. To solve this problem, and get 'almost' random u_i^{B} values, we do the following: we generate the *first* $d-1$ elements of the sum above according to *continuous uniform* RVs on the interval $[a, b]$.

After that we determine the last element according to

$$u_d^{\mathrm{B}} = u^{\mathrm{B}} - \sum_{i=1}^{d-1} u_i^{\mathrm{B}}. \tag{10}$$

In this case the equation (9) will be true, i.e. we get the previously generated value of the key symbol u^{B}.

With the last step of the solution above, the uniformity will be violated for the u_i^{B} elements, which could be a harmful fact in terms of security. We attempt to compensate this effect with the following: let us *hide the position* of the last (i.e. u_d^{B}) element within the vector

$$\mathbf{u}^{\mathrm{B}} = (u_1^{\mathrm{B}}, ..., u_i^{\mathrm{B}}, ..., u_d^{\mathrm{B}}), \tag{11}$$

which has been resulted by the segmentation defined in (9). In practice we *randomly permutate* the indexes of the u_i^{B} elements, which does not affect the correct demodulation.

2) Uniform distribution by normalization: The sum-elements of the u^{B} key symbols to be actually transmitted on the classical channel will be generated according to the following method. We generate uniform RVs, followed by a normalization which realizes the fact that the sum of the elements will be $u^{\mathrm{B}} = \sum_{i=1}^{d} u_i^{\mathrm{B}}$ as in (9).

During this solution, firstly we generate $u_i^{\mathrm{B,pre}}$ continuous uniform RVs on a defined $[a, b]$ interval. In this case to reach that the sum of u_i^{B} elements will be exactly u^{B}, we should normalize the pre-generated $u_i^{\mathrm{B,pre}}$ elements according to

$$u_i^{\mathrm{B}} = u^{\mathrm{B}} \frac{u_i^{\mathrm{B,pre}}}{\sum_{i=1}^{d} u_i^{\mathrm{B,pre}}}. \tag{12}$$

3) Uniform distribution, considering signum: Let us generate information for the input of the classical channel based on the actual $u^{\mathrm{B}} \in [-1, 1]$ symbol to be transmitted in such a way, that we generate d pieces of u_i^{B} elements according to continuous *uniform distribution*.

After this step, if the *sign of the sum* $\sum_{i=1}^{d} u_i^{\mathrm{B}}$ of the generated elements is the same as the sign of the actual u^{B} symbol, the symbol to be transmitted *will have this new value*. In other case each u_i^{B} elements will be multiplied by (-1).

Note that this method can be applied only in case of Binary Phase Shift Keying (BPSK), since the demodulator performs the decision based only on the sign of the received symbol. In this case we 'get back' the $u^{\mathrm{B}} \in [-1, 1]$ elements at the receiver side.

C. Signal level on the classical channel

Let us define a function $\mathrm{C}(.)$ for the elements of vectors $\mathbf{x}^{\mathrm{A}}$ and $\mathbf{x}^{\mathrm{B}}$, which performs *random variable transformation* [8]. The aim of the transformation is to reach a uniform distribution of the raw data elements on the interval $[0, 1]$ in order to *fit the level* of the signal generated based on the raw data to the quantum channel. For the different raw data generation solutions we define different $\mathrm{C}(.)$ functions.

1) Gaussian raw data: The raw data elements are generated according to Gaussian distribution with 0 mean and $\sigma_{x_B}^2$ variance.

In this case we define the following function for the raw data vector elements $\mathbf{x}^{\mathrm{B}}$ at Bob's side

$$\mathrm{C}(x_i^{\mathrm{B}}) = \frac{1}{2}\left(1 + \mathrm{erf}\left(\frac{x_i^{\mathrm{B}}}{\sqrt{2\sigma_{x_B}^2}}\right)\right), \tag{13}$$

where $\mathrm{erf}(x) = \frac{2}{\pi}\int_0^x e^{t^2} dt$.

2) Uniform raw data: We have previously generated uniformly distributed raw data elements on the interval $[a_{\mathrm{u}}, b_{\mathrm{u}}]$. For this case the transformation – which realizes the goal defined above – can be defined by the next steps:

1) The generated raw data elements will be 'shifted' to the 0 'starting position', i.e. we add $-a_{\mathrm{u}}$ to each values.
2) We 'normalize the values' to 1: the values resulted by the first step will be divided by $(b_{\mathrm{u}} - a_{\mathrm{u}})$. That is

$$\mathrm{C}(x_i^{\mathrm{B}}) = \frac{x_i^{\mathrm{B}} - a_{\mathrm{u}}}{(b_{\mathrm{u}} - a_{\mathrm{u}})} \tag{14}$$

Example: let the raw data elements positioned within the interval $[-3, 2]$ uniformly. After executing the first step, the elements will be located in the interval $[0, 5]$. After that the elements will be divided by 5. Finally, each elements will be in the interval $[0, 1]$.

After one of the transformations above, the s_i information elements to be transmitted on the classical channel can be expressed according to the *product*

$$s_i = \mathrm{C}(x_i^{\mathrm{B}})u_i^{\mathrm{B}}. \tag{15}$$

It is visible, that the maximal signal level of the elements u_i^{B} generated after the key-vector partitioning will not be influenced by the $\mathrm{C}(x_i^{\mathrm{B}})$ multiplier, since it can have values only between 0 and 1.

V. Reception on the classical channel

After the previous operations the u^{A} Alice's side received symbol (see Fig. 1) can be expressed as

$$\boxed{u^{\mathrm{A}} = \sum_{i=1}^{d} \frac{s_i}{\mathrm{C}(x_i^{\mathrm{A}})} = \sum_{i=1}^{d} \frac{\mathrm{C}(x_i^{\mathrm{B}})}{\mathrm{C}(x_i^{\mathrm{A}})} u_i^{\mathrm{B}}}. \tag{16}$$

A. The SNR on the classical channel

The SNR on the classical channel is set to $\gamma_{\mathrm{dB}} = \frac{E_s}{N_0} = 40$ dB, where E_s represents the symbol energy, N_0 refers to the spectral power density (in [W/Hz]=[J]) of the Gaussian noise *on the classical channel*. I.e. we add Gaussian noise to the received signal at the classical channel, before demodulation and after the key transmission. This SNR value is large enough to ensure a considerably low bitrate (around 10^{-8}) with the help of BPSK on a classical Additive White Gaussian Noise (AWGN) channel.

From that, N_0 is set to

$$N_0 = \frac{E_s}{10^{\frac{\gamma}{10}}} = \frac{1}{10^{\frac{40}{10}}} = 10^{-4} \text{ [W/Hz]}. \tag{17}$$

B. The SNR on the quantum channel

The measured γ_{q} SNR on the quantum channel can be defined as the ratio of the energies at Alice-side raw data- and the noise samples on the quantum channel, i.e.

$$\gamma_{\mathrm{q}} = \frac{E_{X_{\mathrm{A}}}}{E_{n_{\mathrm{q}}}} = \frac{\sum_{i=1}^{N} \left|x_i^{\mathrm{A}}\right|^2}{\sum_{i=1}^{N} \left|n_i^{(q)}\right|^2}, \tag{18}$$

calculating with the raw data and noise vector elements, where $n_i^{(q)}$ refers to the i-th sample of the noise at the quantum channel. The numerator of the expression above contains the energy amounts in equations (6) and (7) during the calculations.

In order to operate the key distribution with low Symbol-Error-Ratio (SER) and maintain the quantum-nature of the transmission, we should set the maximal $E_{X_{\mathrm{A}}}^{\max}$ transmitter side energy of the x_i^{A} raw data elements.

VI. Simulation

After introducing different generating methods for the raw data and solutions for the key symbol segmentation we provide, we describe the key simulation parameters for the classical and the quantum channels respectively and illustrate the results of the simulation in terms of the SER of the key symbol transmission.

A. Simulation Parameters

We provide the main parameters for the different channels and probability distributions in order the create a simulation scenario, enabling the comparability of the different simulations in terms of the SNR.

1) Parameters on the classical channel: The symbol energy on the classical channel for the BPSK modulation is set to $E_s = 1$ [J], i.e. the signal levels for the two possible symbols are $-\sqrt{E_s}$ and $\sqrt{E_s}$.

We set the interval of the uniform distributed random variables for the break-up of u^{B} vector in (9) as

$$[a_{\mathrm{u}}, b_{\mathrm{u}}] = [-\sqrt{E_{\mathrm{s}}}, \sqrt{E_{\mathrm{s}}}]. \tag{19}$$

2) Parameters on the quantum channel: In order to *reach the desired* γ_{q} SNR during the simulations based on (18) and for a fixed level of $E_{n_{\mathrm{q}}}$ noise energy, we should set the

$$E_{X_{\mathrm{A}}} = \gamma_{\mathrm{q}} E_{n_{\mathrm{q}}} \tag{20}$$

value. In case of different random distributions, different parameters should be set to reach the goal above in terms of the SNR.

For Gaussian distribution the variance of the raw data can be defined based on (6) as

$$\begin{aligned} \sigma_{x_A}^2 &\approx \frac{E_{X_{\mathrm{A}}}}{N} = \frac{\gamma_{\mathrm{q}} E_{n_{\mathrm{q}}}}{N} \\ &\approx \boxed{\gamma_{\mathrm{q}} \sigma_n^2}, \end{aligned} \tag{21}$$

since we know that $E_{n_{\mathrm{q}}} = N\sigma_n^2$.

If the raw data is uniformly distributed, the $\sqrt{E_{X_{\mathrm{A}}}^{\max}}$ limits of the symmetric interval of the raw data can be calculated based on (7) as

$$\begin{aligned} \sqrt{E_{X_{\mathrm{A}}}^{\max}} &= \sqrt{\frac{3E_{X_{\mathrm{A}}}}{N}} = \sqrt{\frac{3\gamma_{\mathrm{q}} E_{n_{\mathrm{q}}}}{N}} = \sqrt{\frac{3\gamma_{\mathrm{q}} N \sigma_n^2}{N}} \\ &= \boxed{\sqrt{3\gamma_{\mathrm{q}} \sigma_n^2}}. \end{aligned} \tag{22}$$

B. Simulation results

At Fig. 2 we provide the results of the simulations during which we have investigated the SER of the key transmission by adjusting the $\gamma_{\mathrm{q,dB}}$ SNR at the quantum channel.

The figure contains SER curves for the cases of two different distributions of the raw data elements (Section III) and by implementing different the key segmentation methods (see IV-B). According to the described raw data generation methods and key symbol segmentation we have six different cases for the key transmission. The SER curves are suggesting that

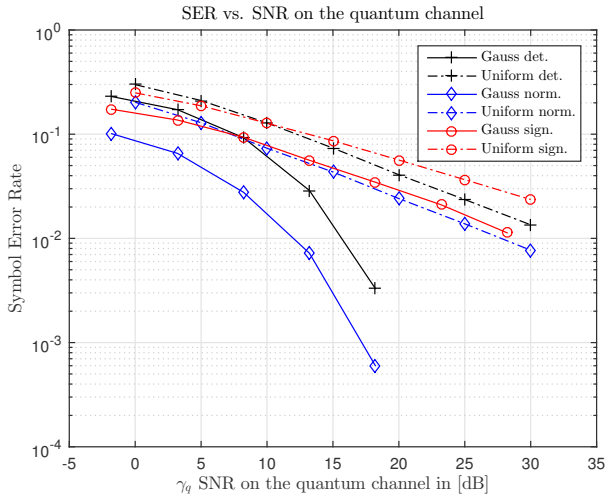

Fig. 2. Illustration of the Symbol-Error-Ratio in case of different Signal-to-Noise-Ratio values at the quantum channel for various raw data distributions and key segmentation methods

the transmission with (truncated) Gaussian raw data elements provides better SER performance in each cases compared to the uniform distribution. In case of the key segmentation the method with normalization (IV-B2) outperforms the two others, i.e. 'det' (IV-B1) and 'sign' (IV-B3), which have intersection points, providing adaptive switching between them in terms of the SNR.

VII. Conclusions

The Continuous-Variable Quantum Key Distribution algorithm proposed in [8] has been implemented first during the evaluating work of the current paper. A MATLAB simulation environment has been implemented to provide a tool for the further investigation of the CVQKD algorithm. Different methods have been introduced to generate the raw data elements and the segmentation of the key symbol in order to provide tools and ideas for the development of the key distribution algorithm.

Acknowledgement

The work reported in this paper has been supported by the Hungarian Scientific Research Fund - OTKA K-112125.

References

[1] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long Distance Continuous-Variable Quantum Key Distribution with a Gaussian Modulation," *Phys. Rev. A 84, 062317*, 2011.

[2] ——, "Analysis of Imperfections in Practical Continuous-Variable Quantum Key Distribution," *Phys. Rev. A 86, 032309*, 2012.

[3] L. R. Allaume, J. Boutros, G. Zmor, and P. Grangier, "Multidimensional reconciliation for continuous-variable quantum key distribution," *quant-ph/07123823, Phys. Rev. A 77, 042325*, 2008.

[4] S. Pirandola, R. Garcia-Patron, S. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," *Phys. Rev. Lett. 102, 050503*, 2009.

[5] S. Pirandola, A. Serafini, and S. Lloyd, "Correlation matrices of two-mode bosonic systems," *Phys. Rev. A 79, 052327*, 2009.

[6] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys. 84, 621*, 2012.

[7] M. Sun, X. Peng, and H. Guo, "An improved two-way continuous-variable quantum key distribution protocol with added noise in homodyne detection," *Journal of Physics B: Atomic Molecular and Optical Physics*, vol. 46, no. 8, 2013.

[8] L. Gyongyosi and S. Imre, "Long-distance Continuous-Variable Quantum Key Distribution With Advanced Reconciliation of a Gaussian Modulation," in *PROCEEDINGS OF SPIE - THE INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING*.