applied sciences

MDPI

Article

Low-Dimensional Reconciliation for Continuous-Variable Quantum Key Distribution

Laszlo Gyongyosi [1,2,3,*] **and Sandor Imre** [2]

[1] School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK
[2] Department of Networked Systems and Services, Budapest University of Technology and Economics, H-1117 Budapest, Hungary; imre@hit.bme.hu
[3] MTA-BME Information Systems Research Group, Hungarian Academy of Sciences, H-1051 Budapest, Hungary
* Correspondence: l.gyongyosi@soton.ac.uk

Received: 12 November 2017; Accepted: 5 January 2018; Published: 9 January 2018

Abstract: We propose an efficient logical layer-based reconciliation method for continuous-variable quantum key distribution (CVQKD) to extract binary information from correlated Gaussian variables. We demonstrate that by operating on the raw-data level, the noise of the quantum channel can be corrected in the low-dimensional (scalar) space, and the reconciliation can be extended to arbitrary dimensions. The CVQKD systems allow an unconditionally secret communication over standard telecommunication networks. To exploit the real potential of CVQKD a robust reconciliation technique is needed. It is currently unavailable, which makes it impossible to reach the real performance of the CVQKD protocols. The reconciliation is a post-processing step separated from the transmission of quantum states, which is aimed to derive the secret key from the raw data. The reconciliation process of correlated Gaussian variables is a complex problem that requires either tomography in the physical layer that is intractable in a practical scenario, or high-cost calculations in the multidimensional spherical space with strict dimensional limitations. To avoid these issues, we define the low-dimensional reconciliation. We prove that the error probability of one-dimensional reconciliation is zero in any practical CVQKD scenario, and provides unconditional security. The results allow for significantly improving the currently available key rates and transmission distances of CVQKD.

Keywords: continuous-variable quantum key distribution; quantum Shannon theory

1. Introduction

The QKD (Quantum Key Distribution) systems represent one of the most important practical applications of quantum information theory [1–18]. The QKD schemes allow for establishing an unconditionally secret communication between distant parties by exploiting the fundamental attributes of quantum mechanics [19–53]. The QKD protocols can be classified into three main classes [1–11,49–53]: DVQKD (Discrete-Variable), CVQKD (Continuous-Variable), and DPR-QKD (Differential Phase Reference) systems. The firstly introduced QKD protocols were based on discrete variables, such as photon polarization. Since the polarization of single photons cannot be encoded and decoded efficiently because of the technological limitations of current physical devices, the CVQKD systems were proposed. In a CVQKD system, the information is encoded on continuous variables by a Gaussian modulation, such as in the position or momentum quadratures of coherent states. In comparison to DVQKD, the modulation and decoding of continuous variables does not require specialized devices and can be implemented efficiently by standard technologies that are available and in widespread use. The CVQKD systems also provide higher secret key rates and higher communication distances. The CVQKD protocols can be further classified into one-way and two-way systems. In a one-way CVQKD system, Alice, the sender transmits her continuous variables to the receiver, Bob, over a quantum channel [9–11]. In a two-way system, Bob starts the communication, Alice adds her internal secret to the received message, and this is then sent back to Bob (e.g., one mode of the coupled beam that is outputted from a beamsplitter is transmitted back to Bob). The two-way CVQKD systems were introduced for practical reasons to exceed the limitations of one-way CVQKD, such as low key rates and short communication distances [1–8]. The two-way CVQKD protocols exploit the benefits of multiple channel uses and allow for the leak of only lower valuable information to the eavesdropper. On the other hand, the achievable distances of one-way CVQKD can be extended by efficient channel-estimation methods [36], which is important since the one-way protocol currently is still the focus of the research, owing to the easy experimental implementation.

The CVQKD schemes use continuous-variable Gaussian modulation, which provably provides optimal key rates against collective attacks at finite-size block lengths [1–11] and also maximizes the mutual information between Alice and Bob. The security of CVQKD has also been proven against collective attacks in the asymptotic regime with infinite block sizes, and against arbitrary attacks in the finite-size regime [9,13,38–40]. One of the most critical points in regard to CVQKD is the post-processing [1–11,47]. The post-processing is aimed to correct the errors of the quantum channel that are cumulated in the raw data. The raw data is a correlated binary bitstring at Alice's and Bob's side, as generated by the random quadrature measurements at the parties. Each quadrature measurement results in a unit in the raw data. The raw data itself is not a secret key; it consists only of the results of the random quadrature measurements. The secret key is a uniformly distributed long binary string that will be combined with the raw data elements, and will be added to the picture only in the stage of logical layer manipulations. The logical layer-based post-processing phase uses purely classical tools: precisely a classical-authenticated communication channel and classical error-correction algorithms. This phase basically does the same in the logical layer as the tomography does in the physical layer, and it consists of two main phases: the reconciliation procedure with several error-correction steps, and privacy amplification.

The aim of reconciliation is to extract as much valuable information from the correlated raw data as possible and to generate an error-free key between Alice and Bob. The privacy amplification operates on the shared, error-corrected common secret to extract the final key between the parties, and the aim of this phase is to reduce to zero the possible knowledge of an eavesdropper from the elements of the key. The implementation of tomography in the physical layer is a complex problem, and it is intractable in a practical scenario. But, well-characterized solutions can be proposed in the logical layer for the same purpose of giving an analogous, and also more valuable, answer to the reconciliation of correlated Gaussian variables than the physical-layer tomography ever could. The theoretical background that makes the logical layer-based reconciliation possible also allow us to view the noisy physical quantum channel as a binary Gaussian channel in the logical layer [9–11]. This has the immediate consequence that very efficient binary error-correction tools can be integrated from the world of traditional communication theory into CVQKD—which would not be available for the physical-layer tomography to extract binary information from the correlated Gaussian variables.

The raw data shared over the quantum channel is noisy, and this must be corrected to distill the final secret key. Since a large amount of raw data bits have to be shared between the parties, the complexity of the post-processing phase is a critical point in CVQKD protocols, and it has to be in order to be as low as possible. The existing logical layer-based solutions require high-complexity calculations in the high-dimensional spherical space for the reconciliation of Gaussian variables [9–11]. Since a complex reconciliation is so undesirable, the aim is to find a more efficient solution in the logical layer. A slice method is a different reconciliation approach, which is also used in the current reconciliation steps of CVQKD for short distances, and can be implemented without spherical operations [41]. Basically, the error correction in the reconciliation phase consists of two phases: First, the binary-channel codes (such as LDPC—Low Density Parity Check, turbo codes, polar codes, etc. [22–35]) that are used for the transmission of the classical bits in the reconciliation phase are corrected. Second, the real Gaussian noise on the received raw-data vector must be corrected, which noise arises from the effect of the quantum channel (i.e., from Eve's optimal Gaussian attack, which is considered in CVQKD protocols [1–11]). In this work, we focus on the second phase of reconciliation, which has a crucial role in CVQKD, since this phase makes it possible to correct the errors that are incurred on the quantum channel and to share an error-free key between Alice and Bob. Since the raw data is formulated by continuous real numbers resulted from quadrature measurements at the parties, the reconciliation problem is analogous to the well-known subject of binary-channel coding that operates on binary-channel codes. It also follows that the complicated and difficult to implement physical-layer tomography can be replaced in the logical level by binary error-correction schemes that are easier to implement. According to a critical security requirement of QKD, in the reconciliation phase, only uniform distribution can be transmitted over the classical channel, otherwise the information theoretic security of the protocol cannot be proven [1–13]. The raw data itself follows Gaussian random distribution because these arise from a Gaussian random source; however, by applying some trivial operations on the raw data units, the desired uniform distribution can be reached, and the reconciliation can be performed with unconditional security, as we will show in detail in Section 3.

A relevant difference of DV and CV protocols is that the physical quantum channel that connects the parties is characterized in a different way. For DVQKD the appropriate channel model is the Binary Symmetric Channel (BSC), which allows the use of the well-known channel-coding and error-correction tools in the post-processing phase. It also follows that for DVQKD there is a clear connection between the characteristics of the quantum channel and the world of traditional communication theory. On the other hand, for a CVQKD system the situation is more complicated, because the proper description of a Gaussian quantum channel requires several physical parameters (transmittance, variance, shot noise, excess noise, etc.) which allows no to draw a clear connection. To solve the situation for one-way CVQKD, the multidimensional reconciliation schemes [9–12] have been introduced, which made possible the conversion of the physical AWGN (Additive White Gaussian Noise) quantum channel to a logical binary AWGN (BAWGN) channel, where the Gaussian random noise arises directly from the quantum-level transmission. Precisely, it works only for low dimensions and the resulted logical channel approximates only a binary Gaussian channel. As the accuracy of the physical-logical channel conversion gets closer to perfect, the resulting logical channel gets closer to a binary Gaussian channel. At low SNRs (Signal-to-Noise Ratio) the capacities of the Gaussian quantum channel and the binary Gaussian channel coincidence, and this is particularly convenient because for low SNRs, the problem of channel conversion can be reduced to the approximation of a binary Gaussian channel. From this follows, that the efficiency of the channel conversion procedure can be described by the relevant parameters of the resulting logical binary channel (such as its variance and capacity). This conversion efficiency has tremendous importance because it also determines the efficiency of the reconciliation process, i.e., the performance of the protocol. In the multidimensional reconciliation the conversion procedure required the use of the spherical space and its sophisticated operations [9–11], which is a complex process. The difficult computational steps of post-processing just cause further slowing down in the very sensitive key rates that are so difficult to establish. These requirements of the reconciliation phase are strongly undesired in a practical CVQKD scenario, so a simpler reconciliation would be desirable—for both one- and two-way systems. The problem of efficient post-processing is more crucial for two-way CVQKD, due to its more complex physical architecture.

To exploit the real potential of two-way CVQKD systems, efficient post-processing is needed. It is still missing, which makes it not possible to attain the true performance of two-way CVQKD. This is the main reason why the theoretical maximum of key rates and ranges cannot be exceeded in the current practical scenarios; however, the protocol in its 'hardware level' is built to be strong, and would be capable of more performance than is currently available. To boost up the performance of the two-way CVQKD protocols over the current limits, we introduce an efficient reconciliation method that makes it possible to increase the key rates and to extend the currently available distance ranges.

The mathematical apparatus that stands behind the multidimensional reconciliation puts a strict upper bound on the available dimensions, and limits its maximum [9–11,42]. The reason is that in higher dimensions the required spherical division operations do not exist. In our scheme, we also eliminate this serious drawback and extend the reconciliation of Gaussian variables to arbitrary high dimensions. The proposed approach also makes possible to get a closer and more precise approximation of the binary Gaussian channel, in comparison to the multidimensional case.

Since the post-processing phase uses the binary form of the continuous variables, in fact, we do not have to decode the Gaussian variables in the multidimensional space. As a corollary, arbitrary high-precision approximation of the logical binary Gaussian channel can be made in the non-spherical space by using considerable dimensions. We exploit it in this work to construct a scalar reconciliation that breaks with the traditions of the previously introduced approaches [9–11,42,46], and uses only the space of scalar variables. The proposed scalar reconciliation is also able to transform the physical Gaussian quantum channel into a logical binary Gaussian channel in two-way CVQKD, and the same benefits can be exploited as in the case of multidimensional reconciliation. However since our scheme is not limited to eight dimensions, an arbitrary precision can be reached in the approximation of the logical binary Gaussian channel. As follows, the accuracy of the conversion between the physical Gaussian quantum channel and the logical Gaussian channel can be improved beyond the current limits. Another issue in the current approaches is the requirement of spherical calculations. To make the existing post-processing approaches more efficient, we have to eliminate the multidimensional operations. The reconciliation of Gaussian variables would be much easier, if we found a solution that would make it possible to extract the final key from the noisy data by simple calculations in the level of scalar space. It immediately follows that this would significantly increase the efficiency of the reconciliation process, and would lead to a negligible complexity and computational power in the error-correction procedure.

In this paper, we define low-dimensional (scalar) reconciliation for CVQKD. It brings significantly higher noise-resistance and information-transmission capability, extended transmission distances, and improved key rates.

The proposed method does the reconciliation of Gaussian variables without the need of any physical-layer tomography or multidimensional operations. We demonstrate the results for two-way CVQKD. The scheme is backward compatible it also can be applied to one-way CVQKD.

The novel contribution of our paper is as follows:

- The reconciliation process of correlated Gaussian variables is a complex problem that requires either tomography in the physical layer that is intractable in a practical scenario, or high-cost calculations in the multidimensional spherical space with strict dimensional limitations.
- To avoid these issues, we propose an efficient logical layer-based reconciliation method for CVQKD to extract binary information from correlated Gaussian variables.
- We demonstrate that by operating on the raw-data level, the noise of the quantum channel can be corrected in the low-dimensional scalar space and the reconciliation can be extended to arbitrary dimensions.
- We prove that the error probability of scalar reconciliation is zero in any practical CVQKD scenario, and provides unconditional security.
- The results allow to significantly improve the currently available key rates and transmission distances of CVQKD.

This paper is organized as follows. In Section 2, preliminary findings are summarized. In Section 3, we introduce the reconciliation scheme. Section 4 provides the theorems and proofs. In Section 5, numerical evidence is proposed. Finally, in Section 6, we conclude the paper. Supplementary Materials are also included, notations are summarized in Table S1.

2. System Model

In comparison to one-way CVQKD protocols, in two-way CVQKD the two uses of the quantum channel lead to superadditive private classical capacity (more precisely, the superadditivity of security threshold leads to a subadditive eavesdropper [1–8,14]), which makes it possible to decrease the amount of valuable information leaked to Eve. The subadditive eavesdropper is a consequence of the multiple uses of the quantum channel. The superadditivity of the security threshold can also be expressed in terms of tolerable excess noise and the channel transmission [1]. In the two-way scenario, Eve perturbs the quantum channel $\mathcal{N}_1$, which causes a noise in the transmission that will have an effect on the success of her second attack. From the two attacks, comparatively lower valuable information will be available to Eve so that she would not have made an attack on $\mathcal{N}_1$. The reason for this is that the amount of valuable information transmitted over $\mathcal{N}_2$ is already decreased by the attack of $\mathcal{N}_1$. More attacks add more noise into the transmission, which also decreases the amount of mutual information between Alice and Bob. With the increased number of channel uses we allow Eve to get as much less valuable information as possible. If Alice encodes her information into the noisy state that is received from $\mathcal{N}_1$, and then sends it back to Bob over $\mathcal{N}_2$, then the parties can achieve the desired phenomenon of superadditivity [1–4]. The amount of valuable information leaked to Eve is also decreased by the multiple uses of the quantum channel. The errors caused by more channel uses can be corrected in the reconciliation phase by traditional error-correction tools. In fact, by utilizing multiple channel uses, we 'set a trap' for Eve, since again and again she will attack the quantum channel. Eve will also simultaneously decrease the amount of eavesdropped information by her actions. The idea works well, because in the post-processing phase the parties can correct the errors caused by Eve, thus, finally, it can be concluded that it was a correct decision to increase the number of channel uses. Of course, if we had perfect amplifiers and ideal devices, then, in theory, it would be possible to completely eliminate Eve from the picture in the asymptotic scenario to make unnecessary the privacy amplification by allowing an infinite amount of channel uses to maximally exploit the superadditivity property (more precisely, the superadditivity of the security-threshold parameter hence the strong subadditivity of Eve). However, in practice it is trivially not possible to circulate over and over the same beam an infinite amount of times, due to the losses and imperfections of the physical devices.

Let us review the data components of the protocol that are needed for the appropriate description of the scalar reconciliation for the two-way CVQKD protocol. Our description will be as detailed as desired for further analysis, and will not take into account the particular description of any components of an experimental protocol. The raw data is generated by the use of noisy Gaussian channels $\mathcal{N}_1$ and $\mathcal{N}_2$, and by the parties' internal secrets. The aim of the quantum-level transmission is to generate two nearly identical classical bitstrings between the parties. All of the quantum-level interactions are closed at this point, and the post-processing phase, which uses the raw data of the parties and a classical authenticated channel, is brought to life. The post-processing phase consists of the processes of reconciliation and privacy amplification. The valuable key will be generated in the reconciliation phase by using the raw data and a random secret. It consists of error-correction phases as well. The privacy amplification is geared toward performing security checks on the elements of the generated key, and it is not part of our description. We will assume reverse reconciliation (RR), which is desirable since the mutual information between Bob and Eve is provably lower than between Alice and Eve [1–7,9–14]. If Bob starts to run the reconciliation phase using his already noisy raw data, then only lower valuable information can be leaked to Eve during the procedure in comparison to if Alice would have started to run the reconciliation, from her ideal raw data (from the perspective of the raw data-level reconciliation, the noise that arises from the first channel use has no relevance, as will be clarified later, and Alice's raw data can be viewed as ideal).

The run of the protocol is sketched as follows. Let us denote Alice's binary raw data by X, and Bob's binary raw data by X', where $|X| = |X'| = N$ units. Alice's raw data is generated by a random quadrature measurement of M_1. Alice's selects two random variables x and p each drawn from a Gaussian distribution, which encodes her position and momentum quadratures and obtains a phase space vector $S_{Alice} = |x_A + ip_A\rangle$. Bob also draws a phase space vector $S_{Bob} = |x_B + ip_B\rangle$. The noisy S'_{Bob} is received by Alice in the first phase via channel $\mathcal{N}_1$ in the beam B_{out}. Alice's raw data is defined as follows:

$$X \equiv M_1(B_{out} + S_{Alice}) = \mathcal{N}_1(S_{Bob}) + S_{Alice}. \tag{1}$$

The outgoing beam A_{out} will contain the other mode of the coupled beam. Bob's raw data is generated by the M_2 random quadrature measurement applied on the beam A_{out}, as:

$$X' \equiv M_2(A_{out}) = B'_{out} + S'_{Alice} = \mathcal{N}_2(\mathcal{N}_1(S_{Bob})) + \mathcal{N}_2(S_{Alice}), \tag{2}$$

where A_{out} contains the noisy version of the second mode of the beam. A detailed description will be given in Section 2.1.

A simplified view of a PM (Prepare-and-Measure: entanglement-free) two-way CVQKD protocol with homodyne measurements M_1, M_2 at the parties and with RR is shown in Figure 1. Alice and Bob are connected by a noisy quantum channel and a classical authenticated channel. The quantum communication is started by Bob. Alice receives Bob's quantum message and then couples it with her quantum message using a BS (Beam Splitter) to create a correlated signal. The first mode of the beam is measured by Alice, using a random quadrature measurement; the second mode is sent back to Bob, who will also apply a random quadrature measurement on the received beam. After the measurements have been performed, the parties inform each other about the used position and momentum quadratures over the classical channel, and discard the irrelevant data. The resulted raw data is a collection of correlated Gaussian variables. Since these binary strings follow Gaussian random distribution, they cannot be transmitted directly over the classical channel. In reverse reconciliation, Bob has to make the probability distribution of his raw data to uniform. He can do this by applying an appropriate function $C(\cdot)$ (will be clarified in Section 3) on his j-th raw data block, as denoted by $\mathbf{X'}_j$. Bob then generates a random key $\mathbf{U}_j$ (the full key vector $\mathbf{K}$ is granulated into several $\mathbf{U}_j$-s), and multiplies it with his raw data $C(\mathbf{X'}_j)$. Alice receives $C(\mathbf{X'}_j)\mathbf{U}_j$, and using her $C(\mathbf{X}_j)$, she computes the noisy $\mathbf{U'}_j$. Next, the errors of the secret key that arise from the noise of the quantum channel will be corrected. This phase is modeled by the scalar reconciliation box at Alice's side. The aim of the scalar reconciliation is to share an error-free key $\mathbf{K}$ between Alice and Bob. From Alice, it requires the correction of the noise on $\mathbf{U'}_j$ to get back Bob's $\mathbf{U}_j$, using only scalar operations without the need of the multidimensional spherical space.

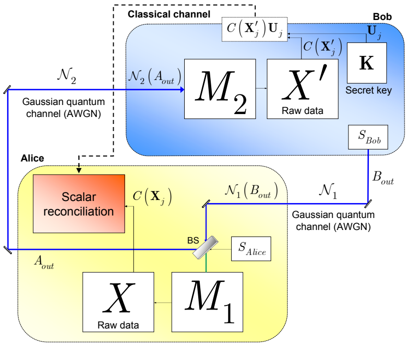


Figure 1. The simplified view of a Prepare-and-Measure (PM)-reverse reconciliation (RR) two-way continuous-variable quantum key distribution (CVQKD) protocol with the scalar reconciliation. The modulated Gaussian variables are sent through a Gaussian quantum channel (AWGN) depicted by $\mathcal{N}_1$ and $\mathcal{N}_2$ (same physical link). The classical channel is depicted by the dashed line. Bob sends S_{Bob} to Alice over $\mathcal{N}_1$. Alice adds to it her secret S_{Alice} by a BS, and applies measurement M_1, which defines her raw data $X = M_1(\mathcal{N}_1(S_{Bob}) + S_{Alice})$. The other mode is sent back to Bob over $\mathcal{N}_2$, who applies M_2, which results in his $X' = M_2(\mathcal{N}_2(\mathcal{N}_1(S_{Bob}) + S_{Alice}))$.

2.1. Physical Coding

In the following description we give a considerable view of the coding of two-way CVQKD, focusing on the contributions of information theory. Let us denote the quadratures of the i-th signal $S_{Alice,i}$ in the phase space $\mathcal{S}_A$ by $x_{A,i}, p_{A,i}$, and the quadratures of Bob's signal $S_{Bob,i}$ in the phase space $\mathcal{S}_B$ by $x_{B,i}, p_{B,i}$, where $x_{A,i}, p_{A,i} \in \mathbb{N}(0, \sigma_\omega^2)$ and $x_{B,i}, p_{B,i} \in \mathbb{N}(0, \sigma_\omega^2)$ are drawn from a Gaussian random distribution with mean $\mu = 0$, and variance σ_ω^2, where σ_ω^2 is the modulation variance [1–10].

The coherent states $S_{Alice,i} = |x_{A,i} + ip_{A,i}\rangle \in \mathcal{S}_A$ and $S_{Bob,i} = |x_{B,i} + ip_{B,i}\rangle \in \mathcal{S}_B$ are encoded by Gaussian modulation with dedicated centers $(x_{A,i}, p_{A,i}) \in \mathcal{S}_A$ and $(x_{B,i}, p_{B,i}) \in \mathcal{S}_B$, respectively (*Note*: Each S_i define a zero-mean, circular symmetric complex Gaussian random variable $\mathcal{C}\mathbb{N}\left(0, \sigma_{S_i}^2\right)$ with variance $\sigma_{S_i}^2 = \mathbb{E}\left[|S_i|^2\right]$ in the phase space $\mathcal{S}$, with i.i.d. real and imaginary components $x_i, p_i \in \mathbb{N}(0, \sigma_\omega^2)$, thus $\sigma_{S_i}^2 = 2\sigma_\omega^2$. The squared magnitude $|S_i|^2$ is exponentially distributed with density $f\left(|S_i|^2\right) = 1\Big/\sigma_{S_i}^2 \exp\left(-|S_i|^2\Big/\sigma_{S_i}^2\right), |S_i|^2 \geq 0$. The two beams are correlated at Alice's BS, which results in a combined signal in the combined phase space $\mathcal{S}_{A\times B}$. The modulation noise $\partial \in \mathcal{C}\mathbb{N}(0, \sigma_\partial^2)$, is precisely centered around $(x_{A,i} + x_{B,i}, p_{A,i} + p_{B,i}) \in \mathcal{S}_{A\times B}$ and $(x_{A,i} - x_{B,i}, p_{A,i} - p_{B,i}) \in \mathcal{S}_{A\times B}$ in $\mathcal{S}_{A\times B}$. After the two beams $S_{Alice,i}$ and $S'_{Bob,i}$ are correlated at a BS at Alice's side, where $S'_{Bob,i}$ is the noisy version of $S_{Bob,i}$, Alice applies a random quadrature measurement M_1 on the first mode of the beam, while the second mode is transmitted back to Bob over quantum channel $\mathcal{N}_2$. Alice's state in the combined phase space $\mathcal{S}_{A\times B}$ is as follows:

$$|\varphi_i\rangle = \left|x_{A,i} + x'_{B,i} + i\left(p_{A,i} + p'_{B,i}\right)\right\rangle \in \mathcal{C}\mathbb{N}\left(0, \sigma_{\varphi_i}^2\right) \in \mathcal{S}_{A\times B}, \tag{3}$$

with Gaussian random quadrature components $\mathbb{N}\left(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2\right)$, where $2\sigma_\omega^2$ is the cumulated modulation variance, $\sigma_{\mathcal{N}_1}^2$ is the variance of $\mathcal{N}_1$, $x'_{B,i}$, $p'_{B,i}$ are Bob's noisy quadratures modified by $\mathcal{N}_1$, while $\sigma_{\varphi_i}^2 = \mathbb{E}\left[|\varphi_i|^2\right]$. Assuming a homodyne measurement M_1, Alice gets an X_i unit of her raw data, which is a binary string. If she measured in the position quadrature basis she obtains:

$$X_i = x_{A,i} + x'_{B,i}, \tag{4}$$

or, if she used the momentum quadrature basis she gets

$$X_i = p_{A,i} + p'_{B,i}. \tag{5}$$

The second mode of the combined signal in $\mathcal{S}_{A\times B}$ is transmitted directly back to Bob over the noisy channel $\mathcal{N}_2$, given as:

$$|\phi_i\rangle = \left|x_{A,i} - x'_{B,i} + i\left(p_{A,i} - p'_{B,i}\right)\right\rangle \in \mathcal{C}\mathbb{N}\left(0, \sigma_{\phi_i}^2\right) \in \mathcal{S}_{A\times B}, \tag{6}$$

with $\mathbb{N}\left(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2\right)$ Gaussian random quadratures, and $\sigma_{\phi_i}^2 = \mathbb{E}\left[|\phi_i|^2\right]$. The Gaussian noise of the quantum channel $\mathcal{N}_2$ defines a noise vector $\Delta_i \in \mathcal{C}\mathbb{N}\left(0, \sigma_{\Delta_i}^2\right) \in \mathcal{S}_{A\times B}$, with noise components $\Delta_{x_i} \in \mathbb{N}\left(0, \sigma_{\mathcal{N}_2}^2\right)$, $\Delta_{p_i} \in \mathcal{C}\mathbb{N}\left(0, \sigma_{\mathcal{N}_2}^2\right)$, which results in the noisy state $|\xi_i\rangle \in \mathcal{S}_{A\times B}$ as follows:

$$|\xi_i\rangle = |\phi_i\rangle + \Delta_i = \left|x'_{A,i} - x''_{B,i} + i\left(p'_{A,i} - p''_{B,i}\right)\right\rangle \in \mathcal{C}\mathbb{N}\left(0, \sigma_{\xi_i}^2\right) \in \mathcal{S}_{A\times B}, \tag{7}$$

with $\mathbb{N}\left(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2 + \sigma_{\mathcal{N}_2}^2\right)$ distributed Gaussian random quadratures, and $\sigma_{\xi_i}^2 = \mathbb{E}\left[|\xi_i|^2\right]$, where $x'_{A,i}$, $p'_{A,i}$ are Alice's noisy quadratures modified by $\mathcal{N}_2$, while $x''_{B,i}$, $p''_{B,i}$ are Bob's noisy quadratures modified by $\mathcal{N}_2$.

In the next phase, Bob applies a random quadrature measurement M_2 (assumed to be homodyne) and gets block Y_i. If he used a position quadrature basis, he gets

$$Y'_i = x'_{A,i} - x''_{B,i}, \tag{8}$$

and for the momentum quadrature basis he obtains:

$$Y'_i = p'_{A,i} - p''_{B,i}. \tag{9}$$

Bob, calibrating his resulted block Y_i' by $2x''_{B,i}$ or $2p''_{B,i}$ (depending on the used quadrature measurement), gets back the noisy version X'_i of Alice's raw data unit X_i as:

$$X_i' = Y'_i + 2x''_{B,i} = x'_{A,i} - x''_{B,i} + 2x''_{B,i} = x'_{A,i} + x''_{B,i} \tag{10}$$

and

$$X_i' = Y'_i + 2p''_{B,i} = p'_{A,i} - p''_{B,i} + 2p''_{B,i} = p'_{A,i} + p''_{B,i}. \tag{11}$$

which is referred as Bob's raw data unit. The nature of the of error of the quantum channel will be characterized in detail in Section 4, however, at this point, we can surmise that the noise of the quantum channel is analogous to the addition of a non-standard Gaussian random noise vector Δ_i to Alice's raw data block X_i.

Alice's and Bob's modes in the combined phase space $\mathcal{S}_{A\times B}$ right after being outputted from the BS are $|\varphi_i\rangle$ and $|\phi_i\rangle$, as shown in Figure 2. Alice obtains the first mode of the beam, $|\varphi_i\rangle$, the second mode $|\phi_i\rangle$ is sent back to Bob. The noise that exists in $\mathcal{S}_{A\times B}$ arises from the modulation noise $\partial \in \mathcal{C}\mathbb{N}(0, \sigma_\partial^2)$ (already included in the quadrature distributions) and the two channel uses, $\mathcal{N}_1$ and $\mathcal{N}_2$. The measurements performed on $|\varphi_i\rangle$ and $|\xi_i\rangle$ result in raw data units $X_i \in \mathbb{N}(0, \sigma_X^2)$ and $X_i' \in \mathbb{N}(0, \sigma_{X'}^2)$. The noise of the first channel changes the Gaussian random distribution of the quadratures from $\mathbb{N}(0, 2\sigma_\omega^2)$ to $\mathbb{N}\left(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2\right)$ in the combined phase space $\mathcal{S}_{A\times B}$, with mean $\mu = 0$, and results X raw data level variance $\sigma_X^2 = \left(2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2\right)$, and where noise variance $\sigma_{\mathcal{N}_1}^2$ arises from the first channel use. The quadratures of the second mode of the coupled beam are also characterized by the same variance, i.e., $|\phi_i\rangle \in \mathcal{C}\mathbb{N}\left(0, \sigma_{\phi_i}^2\right)$. The noise of $\mathcal{N}_2$ transforms $|\phi_i\rangle \in \mathcal{S}_{A\times B}$ into $|\xi_i\rangle \in \mathcal{S}_{A\times B}$ and further modifies the distribution, so finally Bob's received quadratures will follow a Gaussian distribution $\mathbb{N}\left(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2 + \sigma_{\mathcal{N}_2}^2\right)$. The X' raw data level variance is evaluated as $\sigma_{X'}^2 = \left(2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2 + \sigma_{\mathcal{N}_2}^2\right)$, which, in fact, arises from the cumulated Gaussian random noise of $\mathcal{N}_1$ and $\mathcal{N}_2$.

One can recognize that on the raw data level, only the difference of the variance of Alice's and Bob's raw data σ_X^2 and $\sigma_{X'}^2$ has relevance and $\sigma_{\mathcal{N}_1}^2$ vanishes from the picture. This difference is, indeed, $\sigma_{\mathcal{N}_2}^2$. In the level of raw data manipulations Alice's X_i will serve as a reference unit to correct Bob's noisy unit, X'_i. In other words, the first channel use will have no relevance in the raw data-level calculations, hence the noise of $\mathcal{N}_1$ can be excluded from the error-correction process. Precisely, the use of $\mathcal{N}_1$ has only one consequence: it increases the initial variance $2\sigma_\omega^2$ by $\sigma_{\mathcal{N}_1}^2$, which finally results in $\mathbb{N}(0, \sigma_X^2)$ on the level of raw data blocks. In particular, only $\mathcal{N}_2$ will have significance, and, in fact, only the noise of the second channel use has to be corrected in the reconciliation phase. (Note: Throughout the manuscript, the noise will be modeled on the quadrature-level via a real vector).

In the reconciliation phase, our task is to share an error-free secret key between the parties. This requires the raw data-level error-correction of the noise that arises from the quantum-level transmission. First, we review the background of the multidimensional reconciliation, and then we introduce our solution.

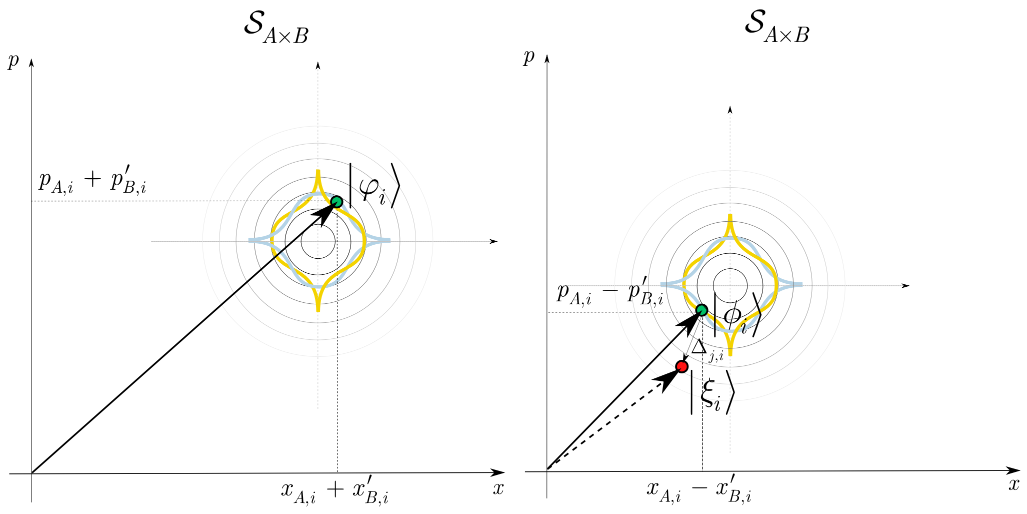

$\mathcal{S}_{A\times B}$
p
$p_{A,i}+p'_{B,i}$
$\left|\varphi_i\right\rangle$
$x_{A,i}+x'_{B,i}$
x
$\mathcal{S}_{A\times B}$
p
$p_{A,i}-p'_{B,i}$
$\left|\phi_i\right\rangle$
$\Delta_{j,i}$
$\left|\xi_i\right\rangle$
$x_{A,i}-x'_{B,i}$
x

Figure 2. The combined signals $|\varphi_i\rangle \in \mathcal{C}\mathbb{N}\left(0,\sigma^2_{\varphi_i}\right)$ and $|\phi_i\rangle \in \mathcal{C}\mathbb{N}\left(0,\sigma^2_{\phi_i}\right)$ in the combined phase space, $\mathcal{S}_{A\times B}$. The modulation noise $\partial \in \mathcal{C}\mathbb{N}(0,\sigma^2_{\partial})$ in $\mathcal{S}_{A\times B}$ is illustrated by the Gaussian curves. The noise $\Delta_i \in \mathbb{N}\left(0,\sigma^2_{\mathcal{N}_2}\right)$ of quantum channel $\mathcal{N}_2$ distorts the distribution of the quadratures from $\mathbb{N}\left(0,2\sigma^2_{\omega}+\sigma^2_{\mathcal{N}_1}\right)$ into $\mathbb{N}\left(0,2\sigma^2_{\omega}+\sigma^2_{\mathcal{N}_1}+\sigma^2_{\mathcal{N}_2}\right)$. Alice's raw data variance is $\sigma^2_X = \left(2\sigma^2_{\omega}+\sigma^2_{\mathcal{N}_1}\right)$, while Bob's raw data variance is $\sigma^2_{X'} = \left(2\sigma^2_{\omega}+\sigma^2_{\mathcal{N}_1}+\sigma^2_{\mathcal{N}_2}\right)$.

2.2. Uniform Distribution in the Spherical Space

In this section we review the background of the multidimensional approaches, and the properties of Gaussian random vectors in the spherical space. The multidimensional reconciliation processes for CVQKD were not implementable without the use of spherical codes and a high-dimensional spherical space.

First, let us clarify how a d-dimensional Gaussian random vector is formulated in the framework of a two-way CVQKD protocol. The outcoming beam from Alice (and Bob) can be regarded as a collection of Gaussian random variables. A standard Gaussian random variable $g \in \mathbb{N}(0,1) \in \mathbb{R}$ is a real variable selected from a Gaussian distribution. A standard Gaussian variable $g \in \mathbb{N}(0,1)$ has probability density function [15,18]:

$$f(g) = \frac{1}{\sqrt{2\pi}} e^{\frac{-g^2}{2}}. \tag{12}$$

A non-standard Gaussian random variable $g^* \in \mathbb{N}\left(\mu,\sigma^2\right) \in \mathbb{R}$ with nonzero mean $\mu \neq 0$, and variance σ^2, can be expressed from $g \in \mathbb{N}(0,1)$ as $g^* = g\sigma + \mu$. A non-standard Gaussian random variable g^* has probability density function:

$$f(g^*) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(g^*-\mu)^2}{2\sigma^2}}. \tag{13}$$

In Alice's raw data, a d-dimensional Gaussian vector

$$\mathbf{X}_j = \left(X_{j,0},\ldots,X_{j,d-1}\right)^T \in \mathbb{N}\left(0,\sigma^2_X\right)_d \in \mathbb{R}^d \tag{14}$$

is a collection of d independent Gaussian random variables $X_{j,0},\ldots,X_{j,d-1}$, where each $X_{j,i}$ is a real variable $\mathbb{R}$ drawn from a Gaussian random distribution $\mathbb{N}\left(0,\sigma^2_X\right)$. Alice's Gaussian vector is referred by $\mathbf{X}_j \in \mathbb{N}\left(0,\sigma^2_X\right)_d \in \mathbb{R}^d$, and its noisy version at Bob's side is denoted by $\mathbf{X'}_j \in \mathbb{N}\left(0,\sigma^2_{X'}\right)_d \in \mathbb{R}^d$. The values of Bob's units are affected by the Gaussian noise that arises from the quantum channel.

First, let us evaluate why the normalized vector structure has importance in the multidimensional scenario. The normalized d-dimensional Gaussian vectors change the probability distribution from Gaussian random to uniform on the d-dimensional unit sphere, Γ^{d-1}. It has a relevance, since only uniform distribution is allowed in the reconciliation phase. The result clearly follows from the Rayleigh law [18], the application of Stirling's formula [19], Gersho's conjecture [22], and Sakrison's result [23], which are connected to the contributions of spherical coding [24].

We formulate d-length blocks $\mathbf{X'}_j = \left(X'_{j,0}, \ldots, X'_{j,d-1}\right)^T \in \mathbb{N}\left(0, \sigma^2_{X'}\right)_d \in \mathbb{R}^d$, where $X'_{j,i} \in \mathbb{N}\left(0, \sigma^2_{X'}\right) \in \mathbb{R}$, for $i \in [d]$. The d-length Gaussian random vector $\mathbf{X'}_j$ has norm $\|\mathbf{X'}_j\|$, mean

$$\mathbb{E}\left[\|\mathbf{X'}_j\|\right] = \sigma_{X'}\sqrt{d - \frac{1}{2}} \tag{15}$$

and variance

$$\operatorname{var}\left[\|\mathbf{X'}_j\|\right] \leq \frac{\sigma^2_{X'}}{2}. \tag{16}$$

We step further from this point. Since the variance of $\mathbf{X'}_j$ is not unit, the covariance matrix $\mathfrak{C}\left(\mathbf{X'}_j\right)$ is not equal to identity, but the random units $X'_{j,i}$ are uncorrelated, so $\mathfrak{C}\left(\mathbf{X'}_j\right)$ is diagonal.

The normalized vector $\mathbf{X'}_{jj} \Big/ \sqrt{d\sigma^2_{X'}}$ with norm $\|\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}\,\|$, can be identified on the unit sphere Γ^{d-1} [18,24], with radius $r = \|\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}\,\|$. The mean of $\|\mathbf{X'}_j\| \Big/ \sqrt{d\sigma^2_{X'}}$ is

$$\mathbb{E}\left[\|\mathbf{X'}_j\| \Big/ \sqrt{d\sigma^2_{X'}}\right] = \sigma_{X'}\sqrt{d - \frac{1}{2}} \Bigg/ \sqrt{d\sigma^2_{X'}}. \tag{17}$$

The vector $\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}$ on the unit sphere Γ^{d-1} is identified as

$$\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}} = r\frac{\mathbf{X'}_j}{\|\mathbf{X'}_j\|} = \frac{\|\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}\, r\|\mathbf{X'}_j}{\|\mathbf{X'}_j\|}. \tag{18}$$

Precisely, the normalized quantity $\|\mathbf{X'}_j\| \Big/ \sqrt{d\sigma^2_{X'}}$ has variance $\operatorname{var}\left[\|\mathbf{X'}_j\| \Big/ \sqrt{d\sigma^2_{X'}}\right] \leq \frac{\sigma^2_{X'}}{2} \Big/ d\sigma^2_{X'}$.

From the spherical symmetry, it follows that if $d \to \infty$, the normalized random vector $\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}$ will be equipped with uniform distribution on Γ^{d-1}. The background of this phenomenon is as follows.

First, for $d \to \infty$, the mean $\mathbb{E}[\cdot]$ of the normalized quantity $\|\mathbf{X'}_j\| \Big/ \sqrt{d\sigma^2_{X'}}$ will tend to one, i.e.,

$$\lim_{d\to\infty} \mathbb{E}\left[\frac{\|\mathbf{X'}_j\|}{\sqrt{d\sigma^2_{X'}}}\right] = \lim_{d\to\infty} \frac{\sigma_{X'}\sqrt{d - \frac{1}{2}}}{\sqrt{d\sigma^2_{X'}}} = 1. \tag{19}$$

Second, the variance $\operatorname{var}[\cdot]$ of $\|\mathbf{X'}_j\| \Big/ \sqrt{d\sigma^2_{X'}}$ will tend to zero,

$$\lim_{d\to\infty} \operatorname{var}\left[\frac{\|\mathbf{X'}_j\|}{\sqrt{d\sigma^2_{X'}}}\right] = \lim_{d\to\infty} \frac{\frac{1}{2}\sigma^2_{X'}}{d\sigma^2_{X'}} = 0. \tag{20}$$

These imply that for $d \to \infty$, the normalized Gaussian random vector $\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}$ becomes *uniformly* distributed on the unit sphere Γ^{d-1}. Third, as the dimension increases the distribution of the norm of $\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}$ (i.e., the radius on Γ^{d-1}) will approximate the Dirac distribution $\mathcal{D}(d)$ [9–11,18], and it will also converge to one, $r = \lim_{d\to\infty} \left\| \mathbf{X'}_j \middle/ \sqrt{d\sigma^2_{X'}} \right\| = 1$. The unit norms of $\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}$ play exactly the role of unit fading-coefficients for a logical binary Gaussian channel, since during the transmissions of the messages generated from $\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}$ the unit norms $r = \left\| \mathbf{X'}_j \middle/ \sqrt{d\sigma^2_{X'}} \right\| = 1$ are also transmitted [11,21].

To be more exact, the unit norms are only approximated and the distribution of the unit norms also depends on d, and as $d \to \infty$, it precisely can be described by the Dirac distribution

$$\mathcal{D}_d(x) = \left(1\big/a\sqrt{\pi}\right)e^{-(x-r)^2\big/a^2}, \tag{21}$$

where $a = 1\Big/\sqrt{d}$ and

$$r = \lim_{d\to\infty} \frac{\|\mathbf{X'}_j\|}{\sqrt{d\sigma^2_{X'}}} = 1. \tag{22}$$

From $\mathcal{D}_d(x)$ it immediately follows, that the unit norms of the normalized random Gaussian vectors gets closer to 1, as d goes to infinity [18]. As follows from these, for low values of d the uniform distribution of $\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}$ cannot be achieved.

In comparison to the multidimensional reconciliation, where the required mathematical operations (the spherical division operator at Alice's side) exist only in $d = 1, 2, 4$, or 8 dimensions [9–11,18], the scalar reconciliation process are also existent for arbitrary high dimensions, which makes possible to give a more closer approximation, however it will not refer to the Dirac distribution. Analyzing the situation if the noisy raw data follows Gaussian random distribution with $\sigma^2_{X'} > 1$, the speed of convergence of the mean $\mathbb{E}\left[\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}\right]$ and variance $\mathrm{var}\left[\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}\right]$ will be lower for any d, in comparison if $\sigma^2_{X'} = 1$ would have hold.

For $\sigma^2_{X'} = 1$, the situation for various dimensions of $\mathbf{X'}_j$ is summarized in Figure 3.

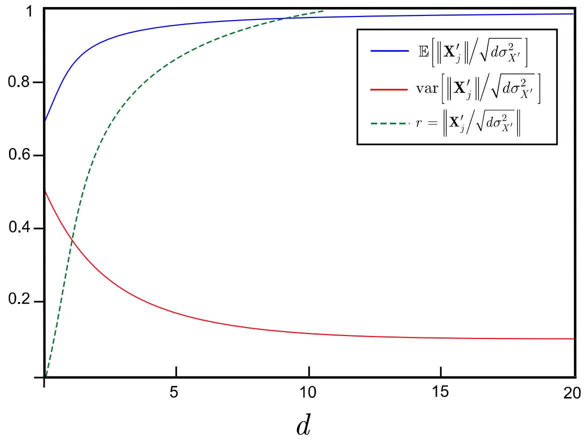


Figure 3. The mean $\mathbb{E}[\cdot]$, variance $\mathrm{var}[\cdot]$ of the normalized quantity $\|\mathbf{X'}_j\|\Big/\sqrt{d\sigma^2_{X'}}$ and the norm $\left\| \mathbf{X'}_j \middle/ \sqrt{d\sigma^2_{X'}} \right\|$ of the normalized Gaussian random vector $\mathbf{X'}_j \Big/ \sqrt{d\sigma^2_{X'}}$. Vector $\mathbf{X'}_j$ is formulated from d number of $X'_{j,i}$ elements of Bob's noisy raw data X'. The approximation of the logical binary Gaussian gets more precise as the norm approaches to one, which requires the use of higher dimensions.

As we have mentioned, the multidimensional approaches are limited in the dimension, specifically, $d = 8$ in [9–11]. In this case, the Gaussian random vectors form the so-called octonions [20]. In the level of Gaussian random raw data, an octonion $\mathrm{O}_j \in \mathbb{R}^8$ is built up from eight units $X_{j,0\ldots j,7} \in \mathbb{N}\left(0, \sigma^2_X\right)$, as:

$$\mathrm{O}_j = X_{j,0}\mathrm{Re} + X_{j,1}\mathrm{Im}_1 + \ldots + X_{j,7}\mathrm{Im}_7, \tag{23}$$

where Re $\in \mathbb{R}$ stands for the real part, while $\text{Im}_i \in \mathbb{C}$, for $i = 1,\ i \leq 7$ identifies the i-th imaginary units, respectively. Bob's noisy O'_j is $\text{O}'_j = X'_{j,0}\text{Re} + X'_{j,1}\text{Im}_1 + \ldots + X'_{j,7}\text{Im}_7$, where $X'_{j,0\ldots7} \in \mathbb{N}(0, \sigma^2_{X'})$. In the multidimensional case the uniformity of the d-dimensional Gaussian random raw data vectors $\mathbf{X}_j \in \mathbb{R}^d$, $d \leq 8$, can be achieved only in the multidimensional spherical space, over the unit sphere Γ^{d-1}. The process requires complex operations and transformations [9–11] that are so undesirable in a practical CVQKD scenario. In comparison to these approaches, our proposed scalar reconciliation uses only simple scalar operations on the raw data, which makes it possible to eliminate the spherical calculations from the reconciliation phase.

3. Low-Dimensional Reconciliation

We start our description from the point at which the quantum states are completely transmitted through the quantum channel from Alice to Bob. At this point, all of the interactions with the quantum channel are closed, and the post-processing phase is being started. First, Alice and Bob exclude from the raw data those measurements that have been performed in different quadratures that result in the N-unit length raw data vectors. Then, formulate N/d number of d-dimensional vectors $\mathbf{X}_j \in \mathbb{R}^d$, $\mathbf{X'}_j \in \mathbb{R}^d$. These quantities are introduced as follows.

3.1. Notations

Let $X \in \mathbb{R}^N$ and $X' \in \mathbb{R}^N$ the N-unit length raw data of Alice and Bob. The d-dimensional vectors $\mathbf{X}_j \in \mathbb{R}^d$ and $\mathbf{X'}_j \in \mathbb{R}^d$, for $j = 0,\ j \leq (N/d) - 1$, of Alice and Bob are defined as:

$$\mathbf{X}_j = \left(X_{j,0}, \ldots, X_{j,d-1}\right)^T \in \mathbb{N}\left(0, \sigma^2_X\right)_d \tag{24}$$

and

$$\mathbf{X'}_j = \left(X'_{j,0}, \ldots, X'_{j,d-1}\right)^T \in \mathbb{N}\left(0, \sigma^2_{X'}\right)_{d'} \tag{25}$$

where

$$X_{j,i} \in \mathbb{N}\left(0, \sigma^2_X\right) \in \mathbb{R} \tag{26}$$

and

$$X'_{j,i} \in \mathbb{N}\left(0, \sigma^2_{X'}\right) \in \mathbb{R} \tag{27}$$

refer to the i-th unit of the j-th vector, respectively. Alice and Bob have to share a common secret by using their correlated raw data. For this purpose, they establish a proper code-alphabet $\mathcal{A} = \{a, b\}$, where $a \in \mathbb{R}$ and $b \in \mathbb{R}$ are two public variables (i.e., Eve also has access to it). In the reverse reconciliation, these will be selected uniformly at random in the form of several $U_j \in \{a, b\}$-s at Bob's side, with $\Pr(a) = \Pr(b) = 0.5$.

A secret d-dimensional key vector $\mathbf{U}_j$ is drawn from a uniform distribution $\mathcal{U}$ and built up from d units, $U_{j,i} \in \mathbb{R}$, as:

$$\mathbf{U}_j \in \mathbb{R}^d : \left(U_{j,0}, \ldots, U_{j,d-1}\right)^T, \text{for } j = 0,\ j \leq (N/d) - 1. \tag{28}$$

The d units $U_{j,i} \in \mathcal{U}$ of $\mathbf{U}_j$ are uniform random variables, and define $U_j \in \mathbb{R}$ as follows:

$$U_j = \textstyle\sum_{i=0}^{d-1} U_{j,i} \in \mathcal{U}. \tag{29}$$

The noisy version of (29), U'_j, is defined as

$$U'_j = \textstyle\sum_{i=0}^{d-1} U'_{j,i}. \tag{30}$$

From (29) follows, that (28) can be rewritten as $\mathbf{U}_j \in \{\mathbf{A}, \mathbf{B}\} \in \mathbb{R}^d$, with vectors $\mathbf{A}, \mathbf{B}$ as:

$$\mathbf{A} : \left(a_{j,0}, \ldots, a_{j,d-1}\right)^T, \left\{\sum_{i=0}^{d-1} a_{j,i} = a\right\}, \mathbf{B} : \left(b_{j,0}, \ldots, b_{j,d-1}\right)^T, \left\{\sum_{i=0}^{d-1} b_{j,i} = b\right\}. \tag{31}$$

As follows, Bob granulates the selected a or b into d number of uniformly random variables $U_{j,i}$, so that the sum of the units will be equal to the selected value.

The full key $\mathbf{K}$ is built up as:

$$\mathbf{K} \in \mathbb{R}^{N/d} : \left(U_0, \ldots, U_{(N/d)-1}\right)^T. \tag{32}$$

Alice and Bob first agree on d. Bob then sends the d blocks of

$$C(\mathbf{X'}_j)\mathbf{U}_j = \left(C(X'_{j,0})U_{j,0}, \ldots, C\left(X'_{j,d-1}\right)U_{j,d-1}\right)^T \in \mathbb{R}^d, \tag{33}$$

for $j = 0, j \leq (N/d) - 1$, over a classical channel. The scalar quantities $C(X_j)$, $C(X'_j)$, and $C(X'_j)U_j$ are evaluated as

$$C(X_j) = \sum_{i=0}^{d-1} C(X_{j,i}) \in \mathbb{R}, C(X'_j) = \sum_{i=0}^{d-1} C(X'_{j,i}) \in \mathbb{R}, \tag{34}$$

and

$$C(X'_j)U_j = \sum_{i=0}^{d-1} C(X'_{j,i})U_{j,i} \in \mathbb{R}, \tag{35}$$

respectively.

Alice receives the d noisy $U'_{j,i}$ units, and by the addition of the d units, and via the application of $C(X_j)$ she computes U'_j as

$$\begin{aligned} U'_j &= \sum_{i=0}^{d-1} U'_{j,i} = C(X'_j)U_j \frac{1}{C(X_j)} \\ &= \left(\sum_{i=0}^{d-1} C(X'_{j,i}) \Big/ \sum_{i=0}^{d-1} C(X_{j,i})\right) \sum_{i=0}^{d-1} U_{j,i}. \end{aligned} \tag{36}$$

Thus, Alice has to make an error-correction to remove the noise from U'_j to get achieve U_j.

3.2. Achieving the Uniform Distribution

In comparison to the multidimensional reconciliation, the scalar reconciliation uses a fundamentally different solution to achieve the uniform distribution of the raw data. While the former is based on sophisticated multidimensional spherical operations, our solution requires only the use of a simple function in the scalar space. In our scheme, the uniform distribution of the correlated raw data units is achieved by the Gaussian Cumulative Distribution Function (CDF) [26,43–45]. Another important difference is that the approximation of the logical binary Gaussian channel can be achieved by arbitrary dimension with arbitrary accuracy, which is justified by the Central Limit Theorem (CLT) [26,43–45].

3.2.1. Gaussian Cumulative Distribution Function

On Alice's and Bob's side, the Gaussian CDF function can be used to reach the uniform distribution of the correlated raw data. Since we assumed reverse reconciliation, let us to start the description from Bob's perspective. Let Bob's raw data unit $X'_{j,i}$ with Gaussian random distribution $\mathbb{N}(0, \sigma^2_{X'})$. The Gaussian CDF-transformation $C(\cdot) : \mathbb{R} \to \mathbb{R}$ for a unit $X'_{j,i}$ is as follows:

$$C(X'_{j,i}) = \frac{1}{2}\left(1 + erf\left(\frac{X'_{j,i}}{\sqrt{2\sigma^2_{X'}}}\right)\right), \text{for } i \in [d], \tag{37}$$

where

$$erf\left(\frac{X'_{j,i}}{\sqrt{2\sigma_{X'}^2}}\right) = \frac{2}{\sqrt{\pi}}\int_0^{X'_{j,i}/\sqrt{2\sigma_{X'}^2}} e^{-t^2}dt \tag{38}$$

is the Gauss error function, and $C\left(X'_{j,i}\right) \in \mathbb{R}$ is a real variable from the range of $[0,1]$, with $\mathcal{U}$ uniform distribution (for a plausible example Section 5). The quantity $C\left(X'_{j,i}\right)$ will be referred as the *CDF*-transformed unit.

Alice also applies the CDF transformation, and takes into account her raw data variance σ_X^2 for the units of $X_{j,i}$ to get $C\left(X_{j,i}\right)$:

$$C\left(X_{j,i}\right) = \frac{1}{2}\left(1 + erf\left(\frac{X_{j,i}}{\sqrt{2\sigma_X^2}}\right)\right), \text{for } i \in [d], \tag{39}$$

and the result of (37) and (39) is the correlated uniform raw data $C\left(X_{j,i}\right) \approx C\left(X'_{j,i}\right)$. In the reconciliation process, only Alice can correct U'_j into U_j, because nobody knows the CDF-transformed raw data units $C\left(X_{j,i}\right)$, except Alice.

For a given $\mathbf{X}_j \in \mathbb{R}^d$, the CDF function $C(\cdot) : \mathbb{R} \to \mathbb{R}$ reads as

$$C\left(\mathbf{X}_j\right) = C\left(X_{j,0}\right), \ldots, C\left(X_{j,d-1}\right) = \frac{1}{2}\left(1 + erf\left(\frac{X_{j,i}}{\sqrt{2\sigma^2}}\right)\right) \in \mathbb{R}, \text{ for } i \in [d], \tag{40}$$

Applying the results for Bob's raw data the CDF-transformed vector is:

$$C\left(\mathbf{X}'_j\right) = C\left(X'_{j,0}\right), \ldots, C\left(X'_{j,d-1}\right) = \frac{1}{2}\left(1 + erf\left(\frac{X'_{j,i}}{\sqrt{2\sigma^2}}\right)\right) \in \mathbb{R}, \text{ for } i \in [d]. \tag{41}$$

The CDF-transformed $C\left(\mathbf{X}_j\right)$, $C\left(\mathbf{X}'_j\right)$ raw data vectors each consist of d real $\mathbb{R}$ variables as:

$$C\left(\mathbf{X}_j\right) = \left(C\left(X_{j,0}\right), \ldots, C\left(X_{j,d-1}\right)\right)^T, C\left(\mathbf{X}'_j\right) = \left(C\left(X'_{j,0}\right), \ldots, C\left(X'_{j,d-1}\right)\right)^T. \tag{42}$$

3.2.2. Central Limit Theorem

In the multidimensional case, the precision of the approximation of the logical binary Gaussian channel (i.e., the quality of the physical-logical channel conversion) was quantified by the Dirac distribution [9–11]. Since in the scalar reconciliation the spherical space is eliminated, a different solution was needed to analyze the accuracy of the conversion between the physical-logical Gaussian channels. Our answer for the problem is the Central Limit Theorem [26,43–45] and a mathematical result from the 19th century—the so-called Lyapunov-condition [26,45]. The accuracy of the physical-logical conversion of scalar reconciliation can be maximized, and it can be made in arbitrary high dimensions, as it is being stated in Lemma 1.

Lemma 1. *The noise variance of the converted logical binary Gaussian channel asymptotically coincidences with the noise variance of the physical quantum channel, which allows to reach the theoretical maximum of the capacity of the converted logical binary channel.*

Proof. Let $X_{j,i} \in \mathbb{R}$ and $X'_{j,i} \in \mathbb{R}$ the j-th units of Alice's and Bob's raw data, respectively. For a d-dimensional vector $\mathbf{U}_j = \left(U'_{j,0}, \ldots, U'_{j,d-1}\right)^T$, the sum of the independent noise $\left\{\delta_{j,0}, \ldots, \delta_{j,d-1}\right\}$ units on the secret noisy key units $U'_{j,i} = U_{j,i} + \delta_{j,i}$ will approximate a zero-mean

Gaussian random variable with mean $\mathbb{E}\left[\delta_{j,i}\right] = \mu_{\delta_{j,i}} = 0$, noise variance $\text{var}\left[\delta_{j,i}\right] = \sigma^2_{\delta_{j,i}}$ (see Sections 3.1 and 3.3 for a detailed derivation) as follows:

$$\begin{gathered}\textbf{CLT}: \frac{1}{\sqrt{\sum_{i=0}^{d-1}\sigma^2_{\delta_{j,i}}}}\delta_j = \frac{1}{\sqrt{\sum_{i=0}^{d-1}\sigma^2_{\delta_{j,i}}}}\left(\sum_{i=0}^{d-1}\delta_{j,i}\right) \to \mathbb{N}(0,1)_d \\ \delta_j = \left(\sum_{i=0}^{d-1}\delta_{j,i}\right) \to \mathbb{N}\left(0, \sum_{i=0}^{d-1}\sigma^2_{\delta_{j,i}}\right) = \mathbb{N}\left(0,\sigma^2_{\delta_{j,i}}\right)_d.\end{gathered} \tag{43}$$

To show that (43) holds for the d-dimensional noise parameter δ_j, we exploit the Lyapunov-condition [26]. Applying the standard mathematical description of the Lyapunov condition [45], let $\mathfrak{L} > 0$, then

$$\lim_{d\to\infty}\frac{1}{\left(\sqrt{\sum_{i=0}^{d-1}\sigma^2_{\delta_{j,i}}}\right)^{2+\mathfrak{L}}}\sum_{i=0}^{d-1}\mathbb{E}\left[\left|\delta_{j,i}\right|^{2+\mathfrak{L}}\right] = 0 \tag{44}$$

is satisfied for any $d \to \infty$, by theory. As follows, the noise on $\mathbf{U}_j \in \mathbb{R}^d$ will converge to

$$\delta_j = \left(\sum_{i=0}^{d-1}\delta_{j,i}\right) \in \mathbb{N}\left(0,\sigma^2_{\delta_j}\right)_d, \tag{45}$$

and the resulting logical channel will be equivalent to a logical binary Gaussian channel with noise variance $\sigma^2_{\delta_j}$. By the same argumentation, the variance of the resulting logical binary Gaussian channel will converge to the variance of the physical Gaussian quantum channel $\sigma^2_{\mathcal{N}_2}$ for $N \to \infty$.

Let again $\mathfrak{L} > 0$, and d is an appropriate dimension for which (44) is satisfied, and let the expected variance of δ_j is $\text{var}\left[\delta_j\right] = \sigma^2_{\mathcal{N}_2}$. Then

$$\lim_{N\to\infty}\frac{1}{\left(\sqrt{\sum_{j=0}^{(N/d)-1}\sigma^2_{\mathcal{N}_2}}\right)^{2+\mathfrak{L}}}\sum_{j=0}^{(N/d)-1}\mathbb{E}\left[\left|\delta_j\right|^{2+\mathfrak{L}}\right] = 0, \tag{46}$$

is satisfied by theory, from which

$$\begin{gathered}\textbf{CLT}: \frac{1}{\sqrt{\sum_{j=0}^{(N/d)-1}\sigma^2_{\mathcal{N}_2}}}\left(\sum_{j=0}^{(N/d)-1}\delta_j\right) \to \mathbb{N}(0,1)_{N/d} \\ \left(\sum_{j=0}^{(N/d)-1}\delta_j\right) \to \mathbb{N}\left(0,\sum_{j=0}^{(N/d)-1}\sigma^2_{\mathcal{N}_2}\right) = \mathbb{N}\left(0,\sigma^2_{\mathcal{N}_2}\right)_{N/d},\end{gathered} \tag{47}$$

follows, which proves the statement. Hence, one can readily recognize that

$$\lim_{N\to\infty}\text{var}\left[\delta_{0\ldots(N/d)-1}\right] = \left(\sigma^2_{\mathcal{N}_2}\right)_{N/d}. \tag{48}$$

To conclude the situation, in (43) and (47) the variances of δ_j and $\sum_{j=0}^{(N/d)-1}\delta_j$, indeed, are not scaled up by d and N/d, which makes possible to convert the physical Gaussian quantum channel to a logical binary Gaussian channel with noise variance $d\sigma^2_{\delta_j} \approx \sigma^2_{\mathcal{N}_2}$ for arbitrary d.

These results allow for one to obtain the lowest noise variance, and hence, the highest SNR of the logical channel that is possible by theory. At the resulting SNR, the capacity of the logical binary Gaussian channel also picks up its maximum. From this, one can immediately conclude, that, in fact, it is a favorable result because the logical channel is indeed a binary Gaussian channel that is equipped with the same capacity at low SNRs (which is the situation in an experimental long-distance scenario) than the physical Gaussian quantum channel. In our solution, the lower bound $\sigma^2_{\delta_j} = \sigma^2_{\mathcal{N}_2}$ is precisely reached and is justified by the Lyapunov-condition, which means that our conversion provides the best approximation that is possible. □

3.2.3. Application

In comparison to the multidimensional approaches, here, one can recognize that these results make no necessary the use of the multidimensional spherical space. The key idea is as follows: do the reconciliation in the scalar space to reduce the problem from Γ^{d-1} of $\mathbb{R}^d$ into $\mathbb{R}$. The main drawback of the multidimensional reconciliation approaches is the use of spherical space Γ^{d-1} of $\mathbb{R}^n$ to achieve the uniform distribution. As we have found in a CVQKD scenario it is not a required condition, and completely can be eliminated. The uniformly distributed elements of $\mathbb{R}^d$ have to be transmitted over the classical authenticated channel, but it *per se*, does not imply that the reconciliation has to be executed in the spherical space. The spherical correction of the errors of the raw data is a completely undesirable and unwanted event in a practical CVQKD, because it would just cause a further decrease in the very fragile, sensitive, and so strenuously established secret key rates. The use of Γ^{d-1} of $\mathbb{R}^d$ served only one purpose in the multidimensional reconciliation: to guarantee the security requirements of the QKD post-processing phase. From this, it immediately can be concluded that the use of spherical space is, in fact, unnecessary, and a mathematically equivalent and more efficient solution exists in the scalar space of $\mathbb{R}$.

One can recognize two improvements in our proposed scheme in comparison to the existing approaches. First, the uniform distribution will be reached by a simple operation, the Gaussian-CDF function applied separately on each unit of the raw data. Second, the approximation of the Gaussian channel will be justified by the CLT, using arbitrary dimensional vectors. As follows, the physical-logical channel conversion can be established with arbitrary high precision, since the $d \leq 8$ limitation has also been eliminated from the picture. To conclude, the spherical space can be replaced by the CDF transformation on the raw data units, and the Dirac distribution can be replaced by the CLT. It is clear now that the existing reconciliation methods require a revision since its application just leads to further slow-down in a practical CVQKD scenario. By these reasons, we drop away the spherical space, and instead of it, use the CDF-transformed units. These improvements allow for very efficient decoding and error-correction, however, this step does not modify any fine property of the code: in other words, it keeps the desired uniform distribution and guarantees the arbitrary high-precision in the approximation of the logical binary Gaussian channel. Finally, we have to emphasize again that the whole reconciliation procedure is implemented through the logical layer only, without any need of physical-layer tomography.

3.3. Run of Scalar Reconciliation

The run of scalar reconciliation (assuming reverse reconciliation) is sketched as follows. Bob divides his N-unit length raw data X' into $n = N/d$ number of d-dimensional vectors $\mathbf{X'}_j = \left(X'_{j,0}, \ldots, X'_{j,d-1}\right)^T \in \mathbb{R}^d$, where d is the length of the vectors measured in units $X'_{j,i}$ in the raw data.

Then, for each $\mathbf{X'}_j$, applies CDF transformation on the units $X'_{j,i} \in \mathbb{R}$ of $\mathbf{X'}_j$, $for\ i = 0,\ i \leq d-1$, $for\ j = 0,\ j \leq (N/d) - 1$. Bob generates $\mathbf{U}_j = \left(U_{j,0} \ldots U_{j,d-1}\right)^T \in \mathbb{R}^d$, $U_{j,i} \in \mathbb{R}$, computes $C(\mathbf{X'}_j)\mathbf{U}_j = \left(C(X'_{j,0})U_{j,0}, \ldots, C\left(X'_{j,d-1}\right)U_{j,d-1}\right)^T$, and sends it to Alice over the classical authenticated channel.

Alice also divides her N-unit length raw data X, into $n = N/d$ number of d-dimensional vectors $\mathbf{X}_j = \left(X_{j,0}, \ldots, X_{j,d-1}\right)^T \in \mathbb{R}^d$, computes the CDF-transformed $C(\mathbf{X}_j) = \left(C(X_{j,0}), \ldots, C\left(X_{j,d-1}\right)\right)^T \in \mathbb{R}^d$ and using (29), (34), and (35) computes as

$$\begin{aligned} U'_j &= C(X'_j)U_j\tfrac{1}{C(X_j)} \\ &= \textstyle\sum_{i=0}^{d-1} X'_{j,i}U_{j,i}\sum_{i=0}^{d-1} U'_{j,i} \\ &= \tfrac{\sum_{i=0}^{d-1} C(X'_{j,i})U_{j,i}}{\sum_{i=0}^{d-1} C(X_{j,i})}. \end{aligned} \tag{49}$$

Next, she corrects the Gaussian noise on U'_j to get U_j. From these she rebuilds the error-free full key

$$\mathbf{K} \in \mathbb{R}^{N/d} : \left(U_0, \ldots, U_{(N/d)-1}\right)^T. \tag{50}$$

3.4. Security

The scalar reconciliation provides unconditional security. It will be demonstrated for reverse reconciliation. The security of scalar reconciliation is guaranteed by the fact that the transmitted $C\left(\mathbf{X'}_j\right)\mathbf{U}_j$ messages follow uniform distribution, and the multiplied $\mathbf{U}_j$ and $\mathbf{X'}_j$ vectors are also uniform and independent.

The following conditional probability holds for each U_j, $U_j = U_{0\ldots1}$ (see also (29),(34) and (35)):

$$\Pr\left(U_j = U_{0\ldots1} | C\left(X'_j\right) U_j\right) = \frac{1}{2}. \tag{51}$$

Since $C\left(\mathbf{X'}_j\right)\mathbf{U}_j$ are uniformly distributed, and also independent [11], it follows that:

$$\Pr\left(C\left(X'_{j,i}\right) = C\left(X'_{j,0}\right) \ldots C\left(X'_{j,N-1}\right)\right) = \frac{1}{N} \tag{52}$$

and

$$\Pr\left(U_j = U_{0\ldots1}\right) = \frac{1}{2}. \tag{53}$$

Since the overall number of d-dimensional $\mathbf{U}_j \in \mathbb{R}^d$ vectors is N/d, the probability that Eve obtains the full key $\mathbf{K}$ is

$$\Pr_{Eve}\left(\mathbf{K} = \left(U_0, \ldots, U_{(N/d)-1}\right)^T\right) = \frac{1}{2^{N/d}}. \tag{54}$$

3.5. Noise on the Data

This section reveals the mathematical description of the noise vector of the Gaussian quantum channel $\mathcal{N}_2$ and its impacts on Bob's raw data and Alice's received secret key. We also can exploit that in the evaluation of the noise vector, only the second channel use $\mathcal{N}_2$ has to be taken in to consideration in the error correction.

The d-dimensional *noise vector* $\Delta_j \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right)_d \in \mathbb{R}^d$ of the Gaussian channel $\mathcal{N}_2$ on the j-th $\mathbf{X'}_j$ is a Gaussian random vector defined as:

$$\Delta_j = \mathbf{X'}_j - \mathbf{X}_j = \left\{\Delta_{j,0}, \ldots, \Delta_{j,d-1}\right\} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right)_d \in \mathbb{R}^d, \tag{55}$$

where $\Delta_{j,i} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right) \in \mathbb{R}$ identifies the Gaussian noise on the i-th unit X_i of $\mathbf{X'}_j$ as:

$$\Delta_{j,i} = X'_{j,i} - X_{j,i} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right) \in \mathbb{R}. \tag{56}$$

The noise vector Δ_j is added to Alice's $\mathbf{X}_j$, hence Bob's noisy $\mathbf{X'}_j$ is:

$$\mathbf{X'}_j = \mathbf{X}_j + \Delta_j \in \mathbb{R}^d. \tag{57}$$

In terms of raw-data vector units, the Gaussian noise vector $\Delta_{j,i}$ is described as follows:

$$X'_{j,i} = X_{j,i} + \Delta_{j,i} \in \mathbb{R}, \tag{58}$$

and (57) can be rewritten as:

$$\begin{aligned}\mathbf{X}'_j &= \left\{X'_{j,0},\ldots,X'_{j,d-1}\right\}\\ &= \left\{X_{j,0}+\Delta_{j,0},\ldots,X_{j,d-1}+\Delta_{j,d-1}\right\}.\end{aligned}\tag{59}$$

In the scalar reconciliation, the error-correction is performed on the level of unit sums $U'_j = \sum_{i=0}^{d-1} U'_{j,i}$ in $\mathbb{R}$ as follows. Alice receives the d-dimensional $C(\mathbf{X}'_j)\mathbf{U}_j$ from Bob, from which she obtains $C(X'_j)U_j$ (see (35)) and divides it by her $C(X_j)$ (see (34)). The effect of Gaussian noise [9] results in a distorted secret $U'_j \in \mathbb{R}$ as:

$$U'_j = \sum\nolimits_{i=0}^{d-1} U'_{j,i} = \frac{\sum_{i=0}^{d-1} C(X'_{j,i})U_{j,i}}{\sum_{i=0}^{d-1} C(X_{j,i})} = \sum\nolimits_{i=0}^{d-1} U_{j,i} + \sum\nolimits_{i=0}^{d-1} \delta_{j,i} = U_j + \delta_j \in \mathbb{R},\tag{60}$$

where $\delta_{j,i}$ is the noise on $U_{j,i}$ (for a plausible example, see Section 5):

$$\delta_{j,i} = \frac{U_{j,i}}{C(X_{j,i})} C(\Delta_{j,i}) \in \mathbb{N}\left(0,\sigma^2_{\delta_{j,i}}\right),\tag{61}$$

where $\sigma^2_{\delta_{j,i}}$ is the variance of the distribution of $\delta_{j,i}$, while $C(\Delta_{j,i})$ is the noise of the CDF-transformed raw data units:

$$C(\Delta_{j,i}) = C(X'_{j,i}) - C(X_{j,i}) \in \mathbb{R},\tag{62}$$

where $C(\Delta_{j,i}) \in \mathbb{N}\left(0,\sigma^2_{C(\Delta_{j,i})}\right)$, and $C(\Delta_j) = C(\mathbf{X}'_j) - C(\mathbf{X}_j) \in \mathbb{R}^d$, with a distribution of $\mathbb{N}\left(0,\sigma^2_{C(\Delta_j)}\right)_d$. The error-corrected U_j can be expressed from the noisy $U'_{j,i}$, as follows:

$$U_j = \sum\nolimits_{i=0}^{d-1} U'_{j,i} - \sum\nolimits_{i=0}^{d-1} \varsigma_{j,i} = U_j - \varsigma_j \in \mathbb{R},\tag{63}$$

where $\varsigma_{j,i} \in \mathbb{N}\left(0,\sigma^2_{\varsigma_{j,i}}\right)$ characterizes the same amount of noise as (61), i.e., and $\varsigma_{j,i} = \delta_{j,i}$, however it is evaluated from the noisy raw-data units $U'_{j,i}$, $C(X'_{j,i})$ as:

$$\varsigma_{j,i} = \frac{U'_{j,i}}{C(X'_{j,i})} C(\Delta_{j,i}) \in \mathbb{R},\tag{64}$$

with $\varsigma_{j,i} \in \mathbb{N}\left(0,\sigma^2_{\varsigma_{j,i}}\right)$. The d-dimensional vector $\mathbf{U}'_j \in \mathbb{R}^d$ can be expressed as:

$$\mathbf{U}'_j = \mathbf{U}_j + \vec{\delta}_j \in \mathbb{R}^d,\tag{65}$$

where the noise vector $\vec{\delta}_j = \left\{\delta_{j,0},\ldots,\delta_{j,d-1}\right\} \in \mathbb{R}^d$ is as follows:

$$\vec{\delta}_j = \frac{\mathbf{U}_j}{C(\mathbf{X}_j)} C(\Delta_j) \in \mathbb{N}\left(0,\sigma^2_{\delta_j}\right)_d = \mathbb{N}\left(0,\sigma^2_{\delta_{j,0},\ldots,\delta_{j,d-1}}\right).\tag{66}$$

According to the CLT, the sum of independent noise on units $U'_{j,i}$ in $\mathbf{U}'_j \in \mathbb{R}^d$ is evaluated by a Gaussian random variable as:

$$\delta_j = \sum\nolimits_{i=0}^{d-1} \delta_{j,i} = \frac{\sum_{i=0}^{d-1} C(\Delta_{j,i})U_{j,i}}{\sum_{i=0}^{d-1} C(X_{j,i})} \in \mathbb{N}\left(0,\sigma^2_{\delta_j} = \sum\nolimits_{i=0}^{d-1} \sigma^2_{\delta_{j,i}}\right).\tag{67}$$

The d-dimensional vector $\mathbf{U}_j \in \mathbb{R}^d$ can be expressed as

$$\mathbf{U}_j = \mathbf{U'}_j - \overset{\rightarrow}{\varsigma}_j \in \mathbb{R}^d, \tag{68}$$

and the noise vector $\overset{\rightarrow}{\varsigma}_j = \left\{ \varsigma_{j,0}, \ldots, \varsigma_{j,d-1} \right\} \in \mathbb{R}^d$ is as follows:

$$\overset{\rightarrow}{\varsigma}_j = \frac{\mathbf{U'}_j}{C(\mathbf{X}_j) + C(\Delta_j)} C(\Delta_j) \in \mathbb{N}\left(0, \sigma^2_{\overset{\rightarrow}{\varsigma}_j}\right)_d. \tag{69}$$

The sum of independent noise on units $U'_{j,i}$ of $\mathbf{U'}_j \in \mathbb{R}^d$ can also be identified as:

$$\varsigma_j = \sum_{i=0}^{d-1} \varsigma_{j,i} = \frac{\sum_{i=0}^{d-1} C(\Delta_{j,i}) U'_{j,i}}{\sum_{i=0}^{d-1} C(X'_{j,i})} = \mathbb{N}\left(0, \sigma^2_{\varsigma_j} = \sum_{i=0}^{d-1} \sigma^2_{\varsigma_{j,i}}\right). \tag{70}$$

From the physical properties of a Gaussian quantum channel [1–11], we know exactly what happens during the transmission of the coherent combined signal from Alice to Bob. The noise on $X'_{j,i}$ has a non-standard Gaussian random distribution $\Delta_{j,i} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right)$.

We have to analyze in detail the properties of the noise vector. The noise vector $\Delta_j \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right)_d \in \mathbb{R}^d$ of $\mathcal{N}_2$ that generates the noisy $\mathbf{X'}_j$ from $\mathbf{X}_j$ is characterized, as follows. First we decompose the noise vector Δ_j into its components:

$$\Delta_j = \mathbf{A}_j \Lambda_j, \tag{71}$$

where matrix $\mathbf{A}_j$ represents a linear transformation in $\mathbb{R}^d$, while Λ_j is a the standard Gaussian noise vector $\Lambda_j \in \mathbb{N}(0,1)_d \in \mathbb{R}^d$. The probability density function of Λ_j is:

$$f(\Lambda_j) = \frac{1}{\left(\sqrt{2\pi}\right)^d} e^{-\frac{\|\Lambda_j\|^2}{2}}, \tag{72}$$

where $\|\Lambda_j\| = \sqrt{\Lambda^2_{j,0} + \ldots + \Lambda^2_{j,d-1}}$ is magnitude, in other words, the Euclidean distance from the origin to $\Lambda_j \in \mathbb{R}^d$. This type of noise exhibits different behavior than the real Gaussian noise of a quantum channel, and it is characterized by the same magnitude $\|\Lambda_j\|$ in every direction. This property is connected to the standard Gaussian random noise, and it cannot be applied in a realistic CVQKD scenario, because it does not properly describe the noise characteristic of the quantum channel. The probability density function of $\Delta_j \in \mathbb{R}^d$ is:

$$f(\Delta_j) = \frac{1}{\left(\sqrt{2\pi}\right)^d \sqrt{\det \mathbf{A}_j \mathbf{A}_j^T}} e^{-\frac{1}{2}\Delta_j^T \left(\mathbf{A}_j \mathbf{A}_j^T\right)^{-1} \Delta_j}, \tag{73}$$

where $\mathbf{A}_j \mathbf{A}_j^T$ stands for the $\mathfrak{C}(\Delta_j)$ covariance matrix of Δ_j, and it analogous of $\sigma^2_{\mathcal{N}_2}$, i.e., in a more precise form $\mathfrak{C}(\Delta_j) = \mathbb{E}\left(\Delta_j \Delta_j^T\right) = \mathbf{A}_j \mathbf{A}_j^T$. The noise on the units $X'_{j,i}$ of $\mathbf{X'}_j$ at Bob's side arises from the quantum-level transmission of the combined phase space states $|\phi_{j,i}\rangle \in \mathcal{S}_{A \times B}$, and vectors $\Lambda_j \in \mathbb{N}(0,1)_d$ and $\Delta_j \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right)_d$ is built up by d components, $\Lambda_{j,i} \in \mathbb{N}(0,1) \in \mathbb{R}$ and $\Delta_{j,i} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right) \in \mathbb{R}$. The error $\Delta_{j,i}$ on the i-th unit $X'_{j,i}$ is as follows:

$$\Delta_{j,i} = \mathbf{A}_{j,i} \Lambda_{j,i}, \text{ for } i = 0, i \leq d-1, \tag{74}$$

where $\mathbf{A}_{j,i}$ is a linear transformation that scales $\Lambda_{j,i}$. The probability density function of $\Lambda_{j,i}$ is:

$$f\left(\Lambda_{j,i}\right) = \frac{1}{\sqrt{2\pi}} e^{-\frac{\|\Lambda_{j,i}\|^2}{2}}, \tag{75}$$

where $\|\Lambda_{j,i}\| = \sqrt{\Lambda_{j,i}^2}$ is the magnitude of $\Lambda_{j,i}$. The probability density function of $\Delta_{j,i}$ is:

$$f\left(\Delta_{j,i}\right) = \frac{1}{\sqrt{2\pi}\sqrt{\det \mathbf{A}_{j,i}\mathbf{A}_{j,i}^T}} e^{-\frac{1}{2}\Delta_{j,i}^T\left(\mathbf{A}_{j,i}\mathbf{A}_{j,i}^T\right)^{-1}\Delta_{j,i}}, \tag{76}$$

where $\mathbf{A}_{j,i}\mathbf{A}_{j,i}^T = \mathbb{E}\left(\Delta_{j,i}\Delta_{j,i}^T\right) = \mathfrak{C}\left(\Delta_{j,i}\right)$.

From $\Lambda_{j,i}$ and $\Delta_{j,i}$, the correction of Bob's noisy secret $\mathbf{U}_j$ can be approached by the units $\left\{U'_{j,0}, \ldots, U'_{j,d-1}\right\}$, because the noise of $\mathcal{N}_2$ is survived in the raw data level and lives also on $U'_{j,i}$, but in a modified form, see (61).

Let us denote by $\left|\phi_{j,i}\right\rangle$, the phase-space representation of Alice's noise-free raw data unit $X_{j,i}$ given by (6), and by $\left|\xi_{j,i}\right\rangle$ the noisy raw data unit $X'_{j,i}$ of Bob, from (7). (State $\left|\phi_{j,i}\right\rangle$ is the second mode of the combined beam, while $\left|\xi_{j,i}\right\rangle$ is its noisy version).

The effect of the real Gaussian noise of the quantum channel is shown in Figure 4. The noise vector $\Delta_j \in \mathbb{N}\left(0, \sigma_{\mathcal{N}_2}^2\right)_d \in \mathcal{S}_{A\times B}$ of the quantum channel is a non-standard Gaussian random vector, which distorts the density. The circles of $\Lambda_{j,i} \in \mathbb{N}(0,1)$ are scaled by $\mathbf{A}_{j,i}$, resulting in ellipses. The magnitude $\|\Delta_{j,i}\|$ of $\Delta_{j,i}$ is not preserved in all directions, which leads to a different density. The x and p quadratures of $\left|\phi_{j,i}\right\rangle \in \mathcal{S}_{A\times B}$ are modified by Δ_x and Δ_p in $\left|\xi_{j,i}\right\rangle \in \mathcal{S}_{A\times B}$.

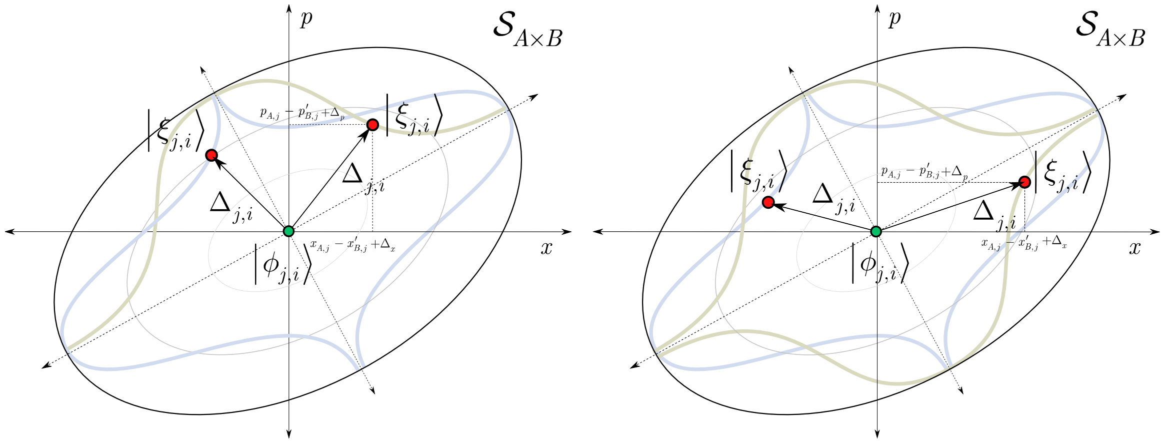

p
$\mathcal{S}_{A\times B}$
$p_{A,j} - p'_{B,j} + \Delta_p$
$\left|\xi_{j,i}\right\rangle$
$\left|\xi_{j,i}\right\rangle$
$\Delta_{j,i}$
$\Delta_{j,i}$
$x_{A,j} - x'_{B,j} + \Delta_x$
$\left|\phi_{j,i}\right\rangle$
x
p
$\mathcal{S}_{A\times B}$
$\left|\xi_{j,i}\right\rangle$
$p_{A,j} - p'_{B,j} + \Delta_p$
$\left|\xi_{j,i}\right\rangle$
$\Delta_{j,i}$
$\Delta_{j,i}$
$x_{A,j} - x'_{B,j} + \Delta_x$
$\left|\phi_{j,i}\right\rangle$
x

Figure 4. The real Gaussian noise of the quantum channel $\mathcal{N}_2$ causes a rotation and rescaled vector in the combined phase space $\mathcal{S}_{A\times B}$ (x: position quadrature, p: momentum quadrature). The magnitude $\|\Delta_{j,i}\|$ of the noise vector $\Delta_{j,i} \in \mathbb{N}\left(0, \sigma_{\mathcal{N}_2}^2\right)$ is not preserved, since the noise characteristic describes an ellipse in the combined phase space.

4. Theorems and Proofs

First, we show that Alice's noisy secret can be corrected in the $\mathbf{v}$ vector space of $\mathbb{R}^d$ by using an error-correction rule based on the apparatus provided by the maximum-likelihood decision [15–19,24,25], which renders unnecessary the use of the spherical space of Γ^{d-1}.

Proposition 1 (Vector reconciliation of correlated Gaussian variables)**.** *The Gaussian noise δ_j on the received vector $\mathbf{U}'_j \in \mathbb{R}^d : \left\{U'_{j,0}, \ldots, U'_{j,d-1}\right\}$ can be corrected in the vector space $\mathbf{v}$* of $\mathbb{R}^d$.

Proof. First, Bob selects the d-dimensional vector $\mathbf{U}_j \in \left\{U_{j,0}, \ldots, U_{j,d-1}\right\} \in \mathbb{R}^d$ where $\sum_{i=0}^{d-1} U_{j,i} = a$ or $\sum_{i=0}^{d-1} U_{j,i} = b$, $U_{j,i} \in \mathcal{U}$ and sends $C(\mathbf{X}'_j)\mathbf{U}_j$ over the classical channel. Alice uses her CDF-transformed raw data $C(\mathbf{X}_j) = \left\{C(X_{j,0}), \ldots, C\left(X_{j,d-1}\right)\right\}$ to obtain $\mathbf{U}'_j \in \mathbb{R}^d$. Since Alice knows a, b and d, she can draw two vectors $\mathbf{A} = (A_0, \ldots, A_{d-1})^T \in \mathbb{R}^d$, with norm $\|\mathbf{A}\| = \sqrt{\sum_{i=0}^{d-1}(A_i)^2}$, where $\left\{\sum_{i=0}^{d-1} A_i = a\right\}$, $A_i \in \mathcal{U}$ and $\mathbf{B} = (B_0, \ldots, B_{d-1})^T \in \mathbb{R}^d$, with $\|\mathbf{B}\| = \sqrt{\sum_{i=0}^{d-1}(B_i)^2}$, where $\left\{\sum_{i=0}^{d-1} B_i = b\right\}$, $B_i \in \mathcal{U}$. She then corrects the noise on $\mathbf{U}'_j$ by the following error-correction rule [15–19]:

$$\mathbf{U}_j = \mathbf{A} : \|\mathbf{U}'_j - \mathbf{A}\| < \|\mathbf{U}'_j - \mathbf{B}\|, \tag{77}$$

$$\mathbf{U}_j = \mathbf{B} : \|\mathbf{U}'_j - \mathbf{A}\| > \|\mathbf{U}'_j - \mathbf{B}\|, \tag{78}$$

where the quantity $\|\mathbf{U}'_j - \mathbf{U}_j\|$, $\mathbf{U}_j \in \{\mathbf{A}, \mathbf{B}\}$ is evaluated as

$$\begin{aligned} \|\mathbf{U}'_j - \mathbf{U}_j\| &= \sqrt{\sum_{i=0}^{d-1}(U'_{j,i} - U_{j,i})^2} = \sqrt{\sum_{i=0}^{d-1}\left(\frac{U_{j,i}}{C(X_{j,i})}C(\Delta_{i,j})\right)^2} \\ &= \sqrt{\sum_{i=0}^{d-1}(\delta_{j,i})^2} = \|\vec{\delta}_j\|, \end{aligned} \tag{79}$$

which precisely coincidences with the norm of the Gaussian noise in (67). However, since Alice does not know Bob's $U_{j,i}$, in (79) an additional noise, Υ_j, also brings up, i.e., $\|\mathbf{U}'_j - \mathbf{U}_j\| = \|\delta_j + \Upsilon_j\|$. The noise vector $\vec{\Upsilon}_j$ with expected variance $\sigma^2_{\vec{\Upsilon}_j}$ is independent from the real noise on $U'_{j,i}$. This problem will be resolved in Theorem 1 and will be shown that this quantity completely vanishes from the picture.

Alice receives the d-dimensional vectors $\mathbf{U}'_j \in \left\{U'_{j,0}, \ldots, U'_{j,d-1}\right\} \in \mathbb{R}^d$, and corrects $\mathbf{U}'_j$ into $\mathbf{U}_j$ and then from the components she rebuilds the full key $\mathbf{K} = \left(U_0, \ldots, U_{(N/d)-1}\right)^T \in \mathbb{R}^{N/d}$. The error-vector $\vec{\delta}_j \in \mathbb{R}^d$ on a given noisy $\mathbf{U}'_j$ is

$$\begin{aligned} \vec{\delta}_j &= \delta_{j,i} = \left(\frac{\mathbf{U}_j}{C(\mathbf{X}_j)}\right)^T C(\Delta_j) \in \mathbb{N}\left(0, \sigma^2_{\vec{\delta}_j} = \mathfrak{C}\left(\left(\frac{\mathbf{U}_j}{C(\mathbf{X}_j)}\right)^T C(\Delta_j)\right)\right)_d \\ &= \mathbb{N}\left(0, \sigma^2_{\delta_{j,i}} = \mathfrak{C}\left(\left(\frac{U_{j,i}}{C(X_{j,i})}\right)^T C(\Delta_{j,i})\right)\right) \in \mathbb{R}^d,\ 0 \le i \le d-1, \end{aligned} \tag{80}$$

The covariance matrix of (80) is expressed as:

$$\mathfrak{C}\left(\left(\frac{\mathbf{U}_j}{C(\mathbf{X}_j)}\right)^T C(\Delta_j)\right) = \mathbb{E}\left(\left(\frac{\mathbf{U}_j}{C(\mathbf{X}_j)}\right)^T C(\Delta_j)\left(\left(\frac{\mathbf{U}_j}{C(\mathbf{X}_j)}\right)^T C(\Delta_j)\right)^T\right) = \left(\sigma^2_{\vec{\delta}_j}\right)_d \tag{81}$$

along with

$$\delta_{j,i} = \left(\frac{U_{j,i}}{C(X_{j,i})}\right)^T C(\Delta_{j,i}) \in \mathbb{N}\left(0, \sigma^2_{\delta_{j,i}} = \mathfrak{C}\left(\left(\frac{U_{j,i}}{C(X_{j,i})}\right)^T C(\Delta_{j,i})\right)\right) \in \mathbb{R}, \tag{82}$$

and (82) is characterized by covariance matrix

$$\mathfrak{C}\left(\frac{U_{j,i}}{C(X_{j,i})}C(\Delta_{j,i})\right) = \mathbb{E}\left(\frac{U_{j,i}}{C(X_{j,i})}C(\Delta_{j,i})\left(\frac{U_{j,i}}{C(X_{j,i})}C(\Delta_{j,i})\right)^T\right) = \sigma^2_{\delta_{j,i}}. \tag{83}$$

The error-corrected $\mathbf{U}_j$ can be expressed as:

$$\mathbf{U}_j = \mathbf{U'}_j - \overrightarrow{\varsigma}_j \in \mathbb{R}^d, \tag{84}$$

where

$$\begin{aligned} \overrightarrow{\varsigma}_j &= \left(\tfrac{\mathbf{U'}_j}{C(\mathbf{X}_j)+C(\Delta_j)} \right)^T C(\Delta_j) \in \mathbb{N}\left(0, \sigma^2_{\overrightarrow{\varsigma}_j} = \mathfrak{C}\left(\left(\tfrac{\mathbf{U'}_j}{C(\mathbf{X}_j)+C(\Delta_j)} \right)^T C(\Delta_j) \right)\right)_d \\ &= \mathbb{N}\left(0, \sigma^2_{\varsigma_j} = \mathfrak{C}\left(\tfrac{U'_{j,i}}{C(X_{j,i})+C(\Delta_{j,i})} C(\Delta_{j,i}) \right)\right) \in \mathbb{R}^d, 0 \le i \le d-1. \end{aligned} \tag{85}$$

The covariance matrix of (85) is as follows:

$$\mathfrak{C}\left(\left(\tfrac{\mathbf{U'}_j}{C(\mathbf{X}_j)+C(\Delta_j)} \right)^T C(\Delta_j) \right) = \mathbb{E}\left(\left(\tfrac{\mathbf{U'}_j}{C(\mathbf{X}_j)+C(\Delta_j)} \right)^T C(\Delta_j) \left(\left(\tfrac{\mathbf{U'}_j}{C(\mathbf{X}_j)+C(\Delta_j)} \right)^T C(\Delta_j) \right)^T \right) = \left(\sigma^2_{\overrightarrow{\varsigma}_j} \right)_d \tag{86}$$

and

$$\varsigma_{j,i} = \frac{U'_{j,i}}{C(X_{j,i}) + C(\Delta_{j,i})} C(\Delta_{j,i}) \in \mathbb{N}\left(0, \sigma^2_{\varsigma_{j,i}} = \mathfrak{C}\left(\frac{U'_{j,i}}{C(X_{j,i}) + C(\Delta_{j,i})} C(\Delta_{j,i}) \right)\right), \tag{87}$$

along with

$$\mathfrak{C}\left(\tfrac{U'_{j,i}}{C(X_{j,i})+C(\Delta_{j,i})} C(\Delta_{j,i}) \right) = \mathbb{E}\left(\tfrac{U'_{j,i}}{C(X_{j,i})+C(\Delta_{j,i})} C(\Delta_{j,i}) \left(\tfrac{U'_{j,i}}{C(X_{j,i})+C(\Delta_{j,i})} C(\Delta_{j,i}) \right)^T \right) = \sigma^2_{\varsigma_{j,i}}. \tag{88}$$

From (82) and (87) the quantities $U_{j,i}$ and $U'_{j,i}$ are evaluated as follows:

$$U_{j,i} = U'_{j,i} - \frac{U'_{j,i}}{C(X'_{j,i})} C(\Delta_{j,i}) = U'_{j,i} - \varsigma_{j,i} \in \mathbb{R}, \tag{89}$$

and

$$U'_{j,i} = \frac{C(X'_{j,i})}{C(X_{j,i})} U_{j,i} = U_{j,i} + \delta_{j,i} \in \mathbb{R}. \tag{90}$$

Let us denote by ν the standard deviation of $\overrightarrow{\delta}_j + \overrightarrow{\Upsilon}_j = \delta_{j,i} + \Upsilon_{j,i}, 0 \le i \le d-1$, which is evaluated from (86) and $\sigma^2_{\overrightarrow{\Upsilon}_j}$ as

$$\nu = \sqrt{\left(\sigma^2_{\overrightarrow{\delta}_j} + \sigma^2_{\overrightarrow{\Upsilon}_j} \right)_d}. \tag{91}$$

The maximum-likelihood-based correction rules can be given in the form of:

$$\mathbf{U}_j = \mathbf{A} : \frac{1}{(\pi 2\nu^2)^{d/2}} e^{-\frac{\|\mathbf{U'}_j - \mathbf{A}\|^2}{2\nu^2}} \ge \frac{1}{(\pi 2\nu^2)^{d/2}} e^{-\frac{\|\mathbf{U'}_j - \mathbf{B}\|^2}{2\nu^2}}, \tag{92}$$

and:

$$\mathbf{U}_j = \mathbf{B} : \frac{1}{(\pi 2\nu^2)^{d/2}} e^{-\frac{\|\mathbf{U'}_j - \mathbf{A}\|^2}{2\nu^2}} \le \frac{1}{(\pi 2\nu^2)^{d/2}} e^{-\frac{\|\mathbf{U'}_j - \mathbf{B}\|^2}{2\nu^2}}. \tag{93}$$

The error probability for the case of decoding vector $\mathbf{U}_j = \mathbf{A}$, is

$$\Pr_e\left(\|\overrightarrow{\delta}_j + \overrightarrow{\Upsilon}_j\|^2 > \|\left(\mathbf{A} + \overrightarrow{\delta}_j + \overrightarrow{\Upsilon}_j\right) - \mathbf{B}\|^2 \right) = \Pr_e\left((\mathbf{A} - \mathbf{B})^T \left(\overrightarrow{\delta}_j + \overrightarrow{\Upsilon}_j \right) < -\frac{\|\mathbf{A} - \mathbf{B}\|^2}{2} \right). \tag{94}$$

For the case of correction of $\mathbf{U}_j = \mathbf{B}$, the error probabilities are evaluated as

$$\Pr_e\left(\|\vec{\delta}_j + \vec{\Upsilon}_j\|^2 > \|\left(\mathbf{B} + \vec{\delta}_j + \vec{\Upsilon}_j\right) - \mathbf{A}\|^2 \right) = \Pr_e\left((\mathbf{B}-\mathbf{A})^T \left(\vec{\delta}_j + \vec{\Upsilon}_j\right) < -\frac{\|\mathbf{B}-\mathbf{A}\|^2}{2} \right). \quad (95)$$

The decision regions can be separated into two hyperplanes $\mathcal{H}_1$ and $\mathcal{H}_2$ along $\mathbf{B} - \mathbf{A}$, which separate $\mathbf{U}_j = \mathbf{A}$ and $\mathbf{U}_j = \mathbf{B}$. In other words, the correction-condition of a given noisy $\mathbf{U'}_j$ is reduced to the following decision problem:

$$\mathbf{U}_j = \begin{cases} \mathbf{A},\ if\ \mathbf{U'}_j \in \mathcal{H}_1, \\ \mathbf{B},\ if\ \mathbf{U'}_j \in \mathcal{H}_2. \end{cases} \quad (96)$$

As follows, by applying the procedure Alice can retrieve $\mathbf{U}_j \in \{\mathbf{A}, \mathbf{B}\}$ from the noisy $\mathbf{U}_j$ in the vector space $\mathbf{v}$ of $\mathbb{R}^d$. From the error-corrected $\mathbf{U}_j$ components, Alice finally rebuilds the full key vector $\mathbf{K} = \left(U_0, \ldots, U_{(N/d)-1}\right)^T \in \mathbb{R}^{N/d}$, which concludes the proof. □

Proposition 1 demonstrated that there is no need for the use of Γ^{d-1} of $\mathbb{R}^d$ in the error correction, however the corrected noise is not precisely a Gaussian. Theorem 1 reveals that the reconciliation process, in fact, does not require vector operations in $\mathbb{R}^d$, and the noise is a real Gaussian noise in the scalar space $\mathbb{R}$.

Theorem 1 (Scalar reconciliation of correlated Gaussian variables)**.** *The Gaussian noise δ_j on the received scalar $U'_j = \sum_{i=0}^{d-1} U'_{j,i}$ can be corrected in $\mathbb{R}$.*

Proof. We exploit that the noise on $U'_{j,i}$-s is $\delta_{j,i} = \frac{U_{j,i}}{C(X_{j,i})} C(\Delta_{j,i}) \in \mathbb{N}\left(0, \sigma^2_{\delta_{j,i}}\right)$, while on the sum of the noise of the d units is a zero-mean Gaussian random variable $\sum_{i=0}^{d-1} \delta_{j,i} \in \mathbb{N}\left(0, \sigma^2_{\delta_j}\right)$, that is justified by the CLT and the Lyapunov-condition. Alice will correct the units in the following form:

$$U'_j = \sum\nolimits_{i=0}^{d-1} U'_{j,i} = \frac{\sum_{i=0}^{d-1} C(X'_{j,i}) U_{j,i}}{\sum_{i=0}^{d-1} C(X_{j,i})} = U_j + \delta_j \in \mathbb{R}. \quad (97)$$

First, expresses the secret vector $\mathbf{U}_j \in \mathbb{R}^d$ as follows:

$$\mathbf{U}_j = x(\mathbf{A} - \mathbf{B}) + \frac{1}{2}(\mathbf{A} + \mathbf{B}), \quad (98)$$

where $x \in \{-0.5, 0.5\} \in \mathbb{R}$ is a scalar. From this, Alice can also rewrite the noisy $\mathbf{U'}_j$ as:

$$\mathbf{U'}_j = x(\mathbf{A} - \mathbf{B}) + \frac{1}{2}(\mathbf{A} + \mathbf{B}) + \vec{\delta}_j. \quad (99)$$

From (99), follows that:

$$\begin{aligned} U'_j &= \sum\nolimits_{i=0}^{d-1} \left(x(A_i - B_i) + \tfrac{1}{2}(A_i + B_i) + \delta_{j,i} \right) \\ &= \sum\nolimits_{i=0}^{d-1} \left(x(A_i - B_i) + \tfrac{1}{2}(A_i + B_i) \right) + \delta_j \\ &= \sum\nolimits_{i=0}^{d-1} U'_{j,i} \\ &= U_j + \tfrac{U_j}{C(X_i)} C(\Delta_j), \end{aligned} \quad (100)$$

where $C(X_j) = \sum_{i=0}^{d-1} C(X_{j,i})$, $C(\Delta_j) = \sum_{i=0}^{d-1} C(\Delta_{j,i})$, $U_j = \sum_{i=0}^{d-1} U_{j,i}$ and $\delta_j = \sum_{i=0}^{d-1} \delta_{j,i}$. In fact, Alice does not have to use all elements from (100), because she can apply a simpler process. For this purpose, she draws a new vector, $\mathbf{d}$:

$$\mathbf{d} = \frac{\mathbf{A}-\mathbf{B}}{\|\mathbf{A}-\mathbf{B}\|}, \tag{101}$$

where $\|\mathbf{A}-\mathbf{B}\| = \sqrt{\sum_{i=0}^{d-1}(A_i - B_i)^2}$ is the effective distance of $\mathbf{A}$ and $\mathbf{B}$. A useful property of vector $\mathbf{d}$ drawn in (101), that any independent noise [15] (i.e., independent from the noise on $\mathbf{U'}_j$) could live only in the orthogonal directions to $\mathbf{d}$, i.e., $(\mathbf{n}_1, \ldots, \mathbf{n}_l) \perp \mathbf{d}$. It immediately follows, that the $\mathbf{n}_1, \ldots, \mathbf{n}_l$ orthogonal directions will have no further importance for Alice in the decoding [15–19]. Since x is a scalar and in (99) the term $\frac{1}{2}(\mathbf{A}+\mathbf{B})$ is a constant, Alice introduces vector $\chi \in \mathbf{v}$ as follows:

$$\chi \equiv \mathbf{U'}_j - \frac{1}{2}(\mathbf{A}+\mathbf{B}) = x(\mathbf{A}-\mathbf{B}) + \vec{\delta}_j. \tag{102}$$

She also draws an orthogonal matrix $\mathbf{M}$, which contains $\mathbf{d}$ and the orthogonal directions $\mathbf{n}_1, \ldots, \mathbf{n}_l$, with unit norm as:

$$\mathbf{M} = \begin{pmatrix} \mathbf{d} \\ \mathbf{n}_1 \\ \mathbf{n}_2 \\ \vdots \\ \mathbf{n}_l \end{pmatrix}. \tag{103}$$

By multiplying $\mathbf{M}$ with χ leads to:

$$\mathbf{M}\chi = \begin{pmatrix} x\|\mathbf{A}-\mathbf{B}\| \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \mathbf{M}\vec{\delta}_j. \tag{104}$$

From (104), it clearly follows that only $x\|\mathbf{A}-\mathbf{B}\|$ and the first component of $\mathbf{M}\vec{\delta}_j$ have relevance in the error-correction process, because all of the other components are orthogonal to $\mathbf{d}$ [15]. Since the evolution of $\mathbf{d}$ is a trivial process on Alice's side, the received $\mathbf{U'}_j$ can be projected by $\mathcal{P}$ onto the direction of $\mathbf{d}$, since all of the valuable information, including the real noise, is carried only by this direction. The projection $\mathcal{P}$ on $\mathbf{U'}_j$ is made by $\mathbf{d}^T\chi$, which then results in:

$$\begin{aligned} \mathcal{P}(\mathbf{U'}_j) &= \mathbf{d}^T\chi \\ &= \left(\tfrac{\mathbf{A}-\mathbf{B}}{\|\mathbf{A}-\mathbf{B}\|}\right)^T (x(\mathbf{A}-\mathbf{B}) + \vec{\delta}_j) \\ &= \mathbf{d}^T\left(\mathbf{U'}_j - \tfrac{1}{2}(\mathbf{A}+\mathbf{B})\right). \end{aligned} \tag{105}$$

The projected vector $\mathcal{P}(\mathbf{U'}_j)$ is analogous to the scalar representation $U_j = \sum_{i=0}^{d-1} U_{j,i}$ in $\mathbb{R}$, and makes it possible to correct the noise in the scalar space $\mathbb{R}$. The received $U'_j = U_j + \delta_j$ has mean $\mu_a = a$ or $\mu_b = b$, and the decision boundary is $\frac{\mu_a+\mu_b}{2}$, which defines a separator in $\mathbb{R}$. According to the previously obtained calculations, (104) can be rewritten as follows:

$$\mathbf{M}\chi = \begin{pmatrix} x\sqrt{\sum_{i=0}^{d-1}(A_i - B_i)^2} \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \delta_j. \tag{106}$$

As follows, only the first component of $\mathbf{M}\vec{\delta}_j$ has relevance in the error-correction, which in particular coincidences with the scalar quantity $\delta_j = \sum_{i=0}^{d-1} \delta_{j,i} = \frac{\sum_{i=0}^{d-1} C(\Delta_{j,i})U_{j,i}}{\sum_{i=0}^{d-1} C(X_{j,i})}$ shown in (79). Putting the pieces together, $\mathcal{P}(\mathbf{U}'_j)$ is evaluated as:

$$\mathcal{P}(\mathbf{U}'_j) = x\sqrt{\sum_{i=0}^{d-1}(A_i - B_i)^2} + \sum_{i=0}^{d-1} \delta_{j,i} \tag{107}$$

which contains all of the sufficient information for the error correction in $\mathbb{R}$, which completes the proof. □

In Theorem 2, the error probability of scalar reconciliation is proposed in an exact form.

Theorem 2. *The error probability* $\Pr(error) = Q\left(\frac{|a-b|}{2}\frac{1}{\eta}\right)$ *of scalar reconciliation depends only on* $|a-b|$, *where* $Q\left(\frac{|a-b|}{2}\frac{1}{\eta}\right) = \Pr\left(\frac{|a-b|}{2}\frac{1}{\eta} < g\right)$ *is the Q-function (tail function), g is a standard Gaussian random variable* $g \in \mathbb{N}(0,1)$ *, and* $\eta = \sqrt{\sigma_{\delta_j}^2} = \sqrt{\sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2}$ *is the standard deviation of the Gaussian noise* δ_j *. The* $\Pr(error)$ *exponentially converges to zero for any* $|a-b| > 2\eta$.

Proof. Let $U_j = \sum_{i=0}^{d-1} U_{j,i}$ from (100), $C(X_j) = \sum_{i=0}^{d-1} C(X_{j,i})$ and $C(\Delta_j) = \sum_{i=0}^{d-1} C(\Delta_{j,i})$. Exploiting the result of Theorem 1, in the scalar reconciliation process Alice decides on the scalar quantity $U'_j = a$, if:

$$\Pr(U_j = a | U'_j) \geq \Pr(U_j = b | U'_j). \tag{108}$$

Similarly, she decides on $U'_j = b$, if:

$$\Pr(U_j = b | U'_j) \geq \Pr(U_j = a | U'_j). \tag{109}$$

Conditioned on a or b, the received U'_j has mean $\mu_a = a$ or $\mu_b = b$, with $\mathbb{N}(\mu_a, \eta^2)$ and $\mathbb{N}(\mu_b, \eta^2)$. Applying the maximum-likelihood-based correction rule [15–19], Alice calculates with the following inequalities:

$$\frac{1}{\sqrt{2\pi\eta^2}} e^{\left(-\frac{(U'_j - a)^2}{2\eta^2}\right)} \geq \frac{1}{\sqrt{2\pi\eta^2}} e^{\left(-\frac{(U'_j - b)^2}{2\eta^2}\right)} \tag{110}$$

and:

$$\frac{1}{\sqrt{2\pi\eta^2}} e^{\left(-\frac{(U'_j - b)^2}{2\eta^2}\right)} \geq \frac{1}{\sqrt{2\pi\eta^2}} e^{\left(-\frac{(U'_j - a)^2}{2\eta^2}\right)}, \tag{111}$$

which then leads to (for a comparison see (77) and (78)):

$$|U'_j - a| < |U'_j - b| \tag{112}$$

and:

$$|U'_j - a| > |U'_j - b|. \tag{113}$$

The received U'_j has mean $\mu_a = a$ or $\mu_b = b$, hence one obtains the following conditional probability for an error event, conditioned on Bob has sent $U_j = a$:

$$\Pr\left(U'_j = \frac{U_j}{C(X_j)} C(\Delta_j) < \frac{\mu_a + \mu_b}{2} \middle| U_j = a \right) = \Pr\left((U'_j - U_j) > \frac{|\mu_a - \mu_b|}{2} \right), \tag{114}$$

where $\frac{|\mu_a - \mu_b|}{2}$ assigns a decision boundary. The tail function $Q\left(\frac{|a-b|}{2}\frac{1}{\eta}\right) = \Pr\left(\frac{|a-b|}{2}\frac{1}{\eta} < g\right)$, where $g \in \mathbb{N}(0,1)$, has exponential decay for any $|a-b| > 2\eta$, hence:

$$\frac{1}{\sqrt{2\pi}\left(\frac{|a-b|}{2}\frac{1}{\eta}\right)} \left(1 - \frac{1}{\left(\frac{|a-b|}{2}\frac{1}{\eta}\right)^2} \right) e^{-\frac{\left(\frac{|a-b|}{2}\frac{1}{\eta}\right)^2}{2}} < Q\left(\frac{|a-b|}{2}\frac{1}{\eta} \right) < e^{-\frac{\left(\frac{|a-b|}{2}\frac{1}{\eta}\right)^2}{2}}, \tag{115}$$

which clearly demonstrates that the error probability of scalar reconciliation exponentially converges to zero. As one can readily obtain from (115), for arbitrary large differences between a and b, $Q\left(\frac{|a-b|}{2}\frac{1}{\eta}\right) \to 0$ [15–17]. Then, by applying the maximum-likelihood decision theory and the Bayes' rule [15–19], for a given U_j, one obtains error probability via the tail function:

$$\begin{aligned} \Pr\left(U'_j < \tfrac{\mu_a+\mu_b}{2} \middle| U_j = a \right) &= Q\left(\tfrac{|a-b|}{2}\tfrac{1}{\eta} \right) \\ &= \Pr\left(\tfrac{|a-b|}{2}\tfrac{1}{\eta} < g \right) \\ &= \Pr(error), \end{aligned} \tag{116}$$

where $g \in \mathbb{N}(0,1)$ is a standard Gaussian random variable such that $Q(x) = \Pr(x < g)$, which clearly demonstrates that $\Pr(error)$ depends only on the distance $|a-b|$ of a and b.

The exponential decay of $\Pr(error)$ is depicted in Figure 5.

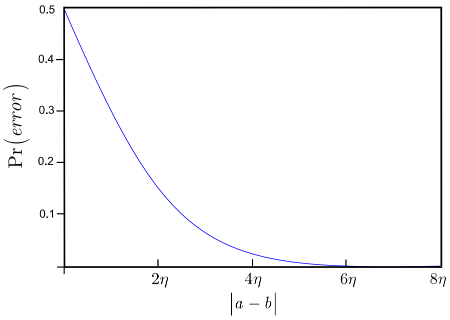


Figure 5. The error probability of the scalar reconciliation process. It converges exponentially to zero as $|a-b| > 2\eta$.

The condition $|a-b| > 2\eta$ can be trivially satisfied by the parties in any practical CVQKD scenario; the proposed results complete the proof. □

5. Numerical Evidence and Noise Model

5.1. Reconciliation Characteristics

In this section, we analyze the performance of the proposed reconciliation for Gaussian modulation, in terms of secret key rates (bits/pulse) and distances. The excess noise $\mathfrak{N}$ of the Gaussian quantum channel is expressed as

$$\mathfrak{N} = \left(\sigma^2_{\omega_E} - 1 \right) (1 - T) T^{-1}, \tag{117}$$

where T is the transmission, and $\sigma^2_{\omega_E}$ is Eve's modulation variance [1]. Assuming reconciliation efficiency $0 \leq \beta \leq 1$, the key rate can be rewritten as

$$R = \beta I(A:B) - \chi(B:E), \tag{118}$$

where $I(A:B)$ is the mutual information between Alice and Bob, while $\chi(B:E)$ is the Holevo information between Bob and Eve, respectively, with relation

$$\chi(B:E) < \chi(A:E), \tag{119}$$

where $\chi(A:E)$ is the Holevo information between Alice and Eve at a direct reconciliation [1–13]. At a given SNR, the mutual information of Alice and Bob is [1–8]

$$\chi(A:B) \geq 1/2 \log_2(1+\text{SNR}), \tag{120}$$

where

$$\text{SNR} = \sigma^2_{\phi} \Big/ \sigma^2_{\mathcal{N}_2}, \tag{121}$$

where σ^2_{ϕ} is the transmit signal's variance, $\sigma^2_{\mathcal{N}_2}$ is the variance of $\mathcal{N}_2$, which has parameters that can be calculated from T and $\mathfrak{N}$. In Figure 6a the $d\sigma^2_{\delta_j}$ quantities of the converted logical binary Gaussian channel for various dimensions are shown. As depicted by the red line, the Lyapunov-condition can be exploited to get variance

$$\lim_{N/d \to \infty} d\text{var}\left[\delta_{0\ldots N/d}\right] = \text{var}\left[\delta_{0\ldots N/d}\right] \approx \left(\sigma^2_{\mathcal{N}_2}\right)_d \tag{122}$$

for arbitrary d to maximize the SNR value,

$$\text{SNR} = \sigma^2_{X} \Big/ \sigma^2_{\delta_j} \tag{123}$$

of the converted logical channel. As depicted in Figure 6b, for $d \to \infty$, the efficiency converges to one, $\beta \to 1$, because the noise perfectly converges to a zero-mean Gaussian random variable.

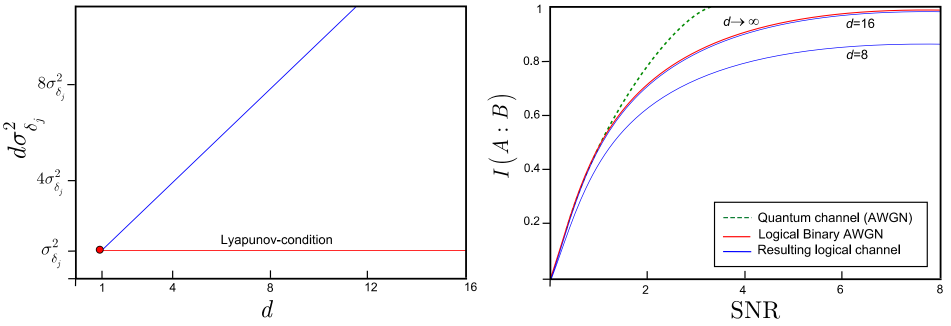


Figure 6. (**a**) The Signal-to-Noise Ratio (SNR) of the resulting logical binary channel is maximized by the Lyapunov-condition (red line). It makes possible to convert the physical Gaussian quantum channel to a logical channel with the same noise variance for arbitrary d. For the blue line the Lyapunov-condition is not satisfied. (**b**) The capacity of the logical channel for various dimensions. At low SNRs the capacity of the physical Gaussian quantum channel (dashed line) coincidences with the capacity of the binary Gaussian channel (red). For $d = 16$, the capacity of the logical channel is very close to the capacity of a binary Gaussian channel, and at low SNRs it perfectly coincidences with the capacity of the Gaussian quantum channel. The reconciliation efficiency at $d = 16$ is $\beta = 0.97$. The curves for lower d-s do not exist because the resulting logical channels are not Gaussian, since the Lyapunov-condition is not satisfied in the low-regimes.

The numerical analysis uses a two-way CVQKD protocol, with homodyne measurements. The parameters are as follows. Excess noise $\mathfrak{N} = 0.015$, $T = 0.8$, variance $\sigma_X^2 = 1.06$, channel correlation $n_C = 0.5$, which parameter describes the correlation of the Gaussian attacks of Eve in the range of $0 \leq n_C \leq 1$ [7,8]. (*Note*: If $n_C = 0$, there is no correlation between her attacks of $\mathcal{N}_1$ and $\mathcal{N}_2$ [7,8]).

In Figure 7 the SNR of the logical binary Gaussian are depicted for various dimensions.

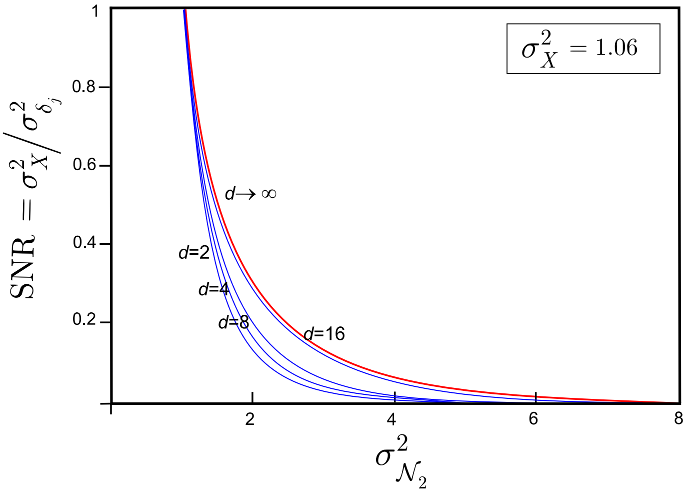


Figure 7. The SNRs of the logical channel at variance $\sigma_X^2 = 1.06$. As the dimension increases the variance of the logical channel reaches the variance of the physical quantum channel. At $d = 16$ the variances perfectly coincidence.

The performance of scalar reconciliation is summarized in Figure 8. The performance of the simulated protocol without scalar reconciliation with reconciliation efficiency $\beta = 0.9$, is depicted by the blue curve [7,8]. At $d = 16$, improved the reconciliation efficiency to $\beta = 0.97$, which resulted in significantly higher transmission distances and secret key rates.

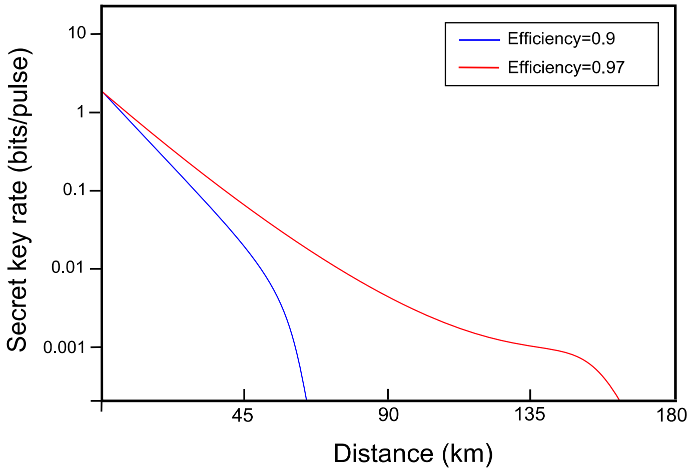


Figure 8. The performance of scalar reconciliation in two-way PM-RR continuous-variable quantum key distribution (CVQKD) at $d = 16$ (homodyne measurement at both sides). Excess noise: $\mathfrak{N} = 0.015$, transmittance: $T = 0.8$, Eve's variance $\sigma_{\omega_E}^2 = 1.06$, channel correlation: $n_C = 0.5$, signal variance $\sigma_\phi^2 = 20$.

The scalar reconciliation applied on the two-way CVQKD protocol resulted in approximately 160 km of achievable transmission distance (for the computations of the secret key rate, and the detection parameters, see the derivations of [1,7,8]). The results indicate that the range of the current two-way CVQKD without our post-processing technique can be significantly extended, and the maximal 80.5 km range of the current one-way CVQKD systems [12] can be doubled, and almost tripled compared with existing two-way CVQKD systems [7,8]. The reason behind the phenomenon is the possibility of the conversion of the Gaussian quantum channel to a logical binary Gaussian channel, similar to the multidimensional reconciliation approaches developed for one-way CVQKD.

The favorable properties of the multidimensional solutions are preserved here, however the proposed scalar reconciliation does not require any multidimensional spherical calculations [9–11] and can be extended to arbitrary high dimensions thanks to the fact that it completely eliminates the spherical operations. From the use of higher dimensions, a more precise approximation of the logical binary Gaussian channel has also become available which resulted in significantly higher reconciliation efficiency in comparison to current two-way CVQKD reconciliation methods.

The proposed scalar reconciliation is available at low SNRs, and the transmission ranges of experimental long-distance CVQKD can significantly be improved because at low SNRs the capacity of the logical binary Gaussian channel coincidences with the capacity of the Gaussian quantum channel, and the logical channel resulted from the conversion can approximate it with arbitrary-high precision.

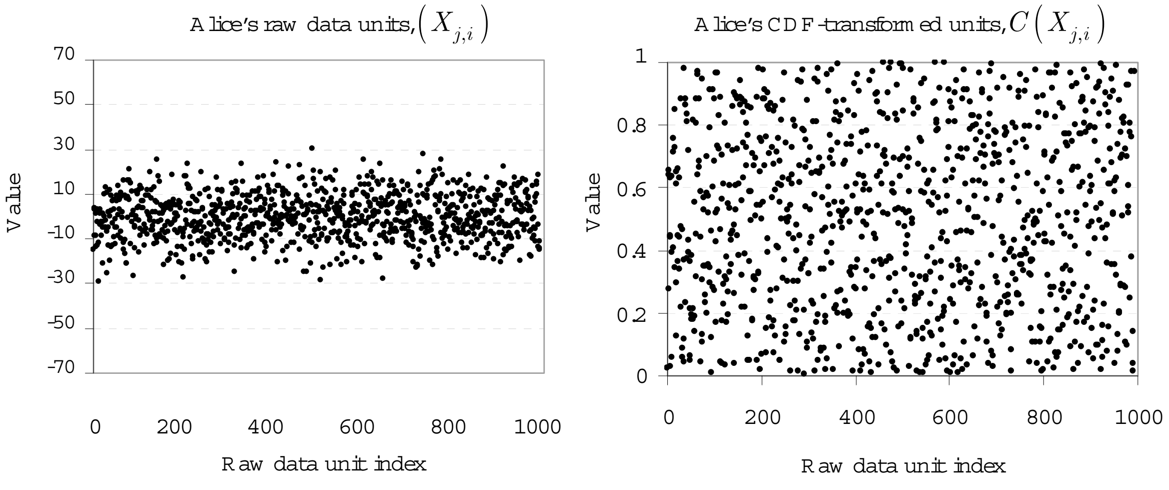
5.2. Noise Analysis

5.2.1. Noise on the Raw Data

The following example demonstrates the change of behavior of the probability distribution of raw data units and the CDF-transformed units, and serves only demonstration purposes.

For an illustrative example, let $N = 1000$ units, the amount of sample raw data units $X_{j,i}$, $X'_{j,i}$ (the units are resulted from random quadrature measurements) taken from Alice's and Bob's raw data, respectively. The Gaussian random units $X_{j,i}$ are characterized with zero mean and variance $\sigma_X^2 = 100$.

In Figure 9a, the distribution of the $X_{j,i}$ Gaussian random raw data units is shown. Figure 9b depicts the result of the $C(\cdot)$ Gaussian CDF function applied on $X_{j,i}$. The Gaussian random behavior is eliminated and is changed into uniform.



(**a**) (**b**)

Figure 9. (**a**) The distribution of Alice's raw data units. The units follow Gaussian random distribution; (**b**) The distribution of the Cumulative Distribution Function (CDF)-transformed units. The probability distribution has changed into uniform in the range of $[0,1]$.

The distribution of the Gaussian noise vector $\Delta_{j,i} \in \mathbb{N}\left(0, \sigma_{\mathcal{N}_2}^2\right)$ of the quantum channel $\mathcal{N}_2$, at $\sigma_{\mathcal{N}_2}^2 = 4$ is shown in Figure 10.

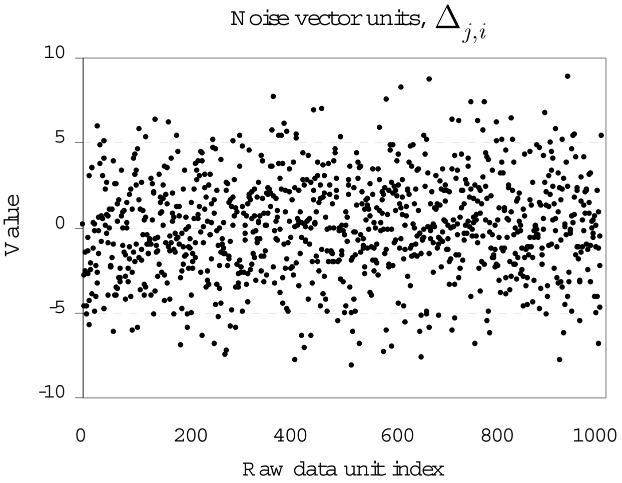


Figure 10. The distribution of the units of the noise vector of the Gaussian quantum channel. The noise affects the combined state in the phase space and the resulting raw data units on Bob's side.

At Bob's side, the received noisy units $X'_{j,i}$ and the CDF-transformed $C\left(X'_{j,i}\right)$ units have a modified distribution with variance $\sigma^2_{X'} = \sigma^2_X + \sigma^2_{\mathcal{N}_2} = 104$, as depicted in Figure 11. The Gaussian noise on the units is added by $\Delta_{j,i} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right)$.

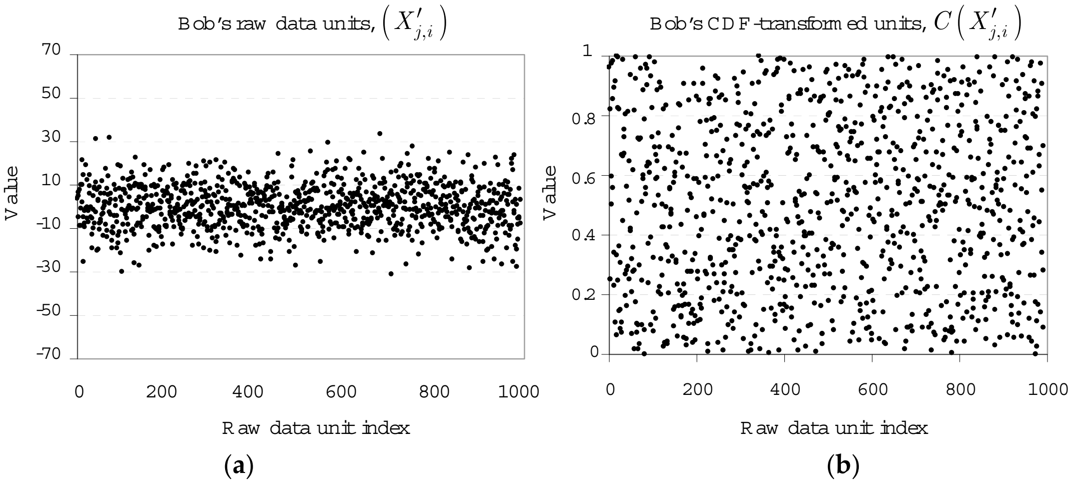


Figure 11. (**a**) The distribution of the noisy raw data units on Bob's side; (**b**) The CDF-transformed raw data units have uniform distribution in $[0, 1]$.

This example showed that the uniform distribution of the Gaussian random raw data could be achieved by trivial operations, without any multidimensional calculations or coding.

5.2.2. Noise on the Random Secret

This example demonstrates that the noise $\delta_j = \frac{\sum_{i=0}^{d-1} C(\Delta_{j,i}) U_{j,i}}{\sum_{i=0}^{d-1} C(X_{j,i})}$ on the secret $U'_j = \sum_{i=0}^{d-1} U'_{j,i}$ is inherited from the Gaussian quantum channel and by applying the Central Limit Theorem (CLT), the noise of the logical binary channel can be approximated by a Gaussian random variable $\delta_j = \sum_{i=0}^{d-1} \delta_{j,i} \in \mathbb{N}\left(0, \sigma^2_{\delta_j}\right)$.

Let $N = 1000$ units, the amount of sample raw data units $X_{j,i}$, $X'_{j,i}$. The quantity $C(\Delta_j) = C(\mathbf{X'}_j) - C(\mathbf{X}_j)$ measures the difference of $C(\mathbf{X'}_j)$ and $C(\mathbf{X}_j)$, i.e., the noise of Bob's

CDF-transformed data. Let $\mathbf{X}_j \in \mathbb{N}\left(0, \sigma_X^2 = 100\right)$ and $\mathbf{X'}_j \in \mathbb{N}\left(0, \sigma_{X'}^2 = 104\right)$. The example uses an $d = 16$ dimensional approximation.

The distribution of the error $C\left(\Delta_{j,i}\right)$ of the CDF-transformed raw data units $C\left(X'_{j,i}\right), C\left(X_{j,i}\right)$ are depicted in Figure 12.

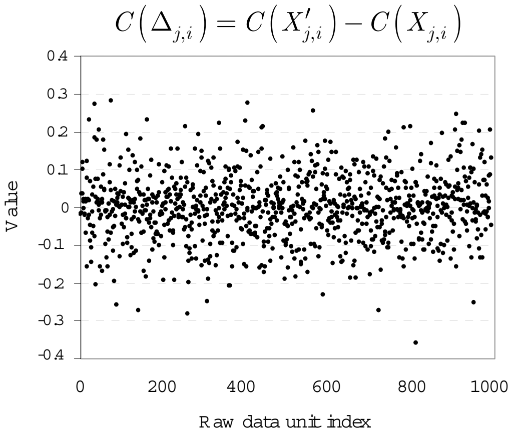


Figure 12. The distribution of the error $C\left(\Delta_{j,i}\right) = C\left(X'_{j,i}\right) - C\left(X_{j,i}\right)$ on the CDF-transformed raw data units.

In Figure 13a the ratio $C\left(X'_{j,i}\right)/C\left(X_{j,i}\right)$ of the CDF-transformed units is shown in Figure 13a. In the ideal (noise-free) case the ratio equals to 1. In Figure 13b the distribution of the quantity $C\left(\Delta_{j,i}\right)/C\left(X_{j,i}\right)$ is shown.

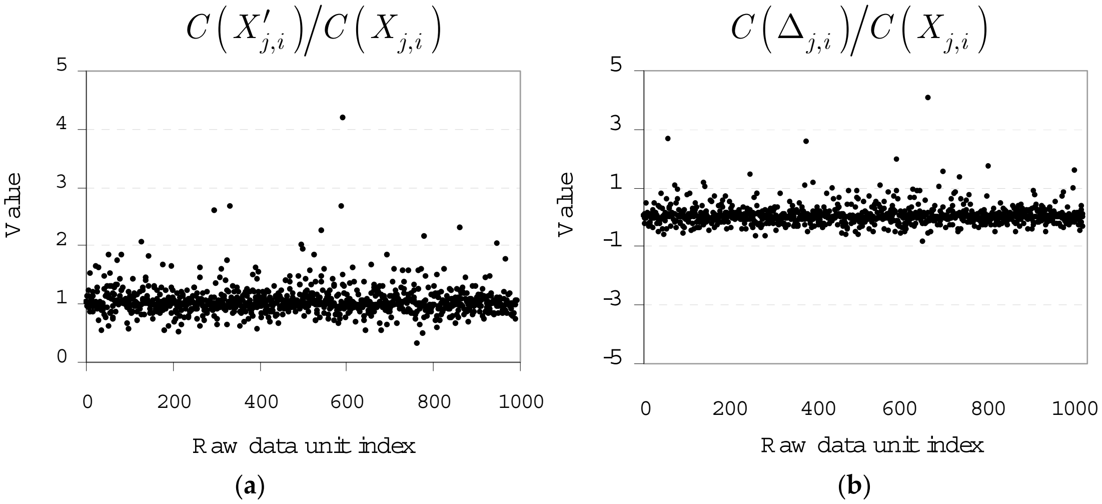
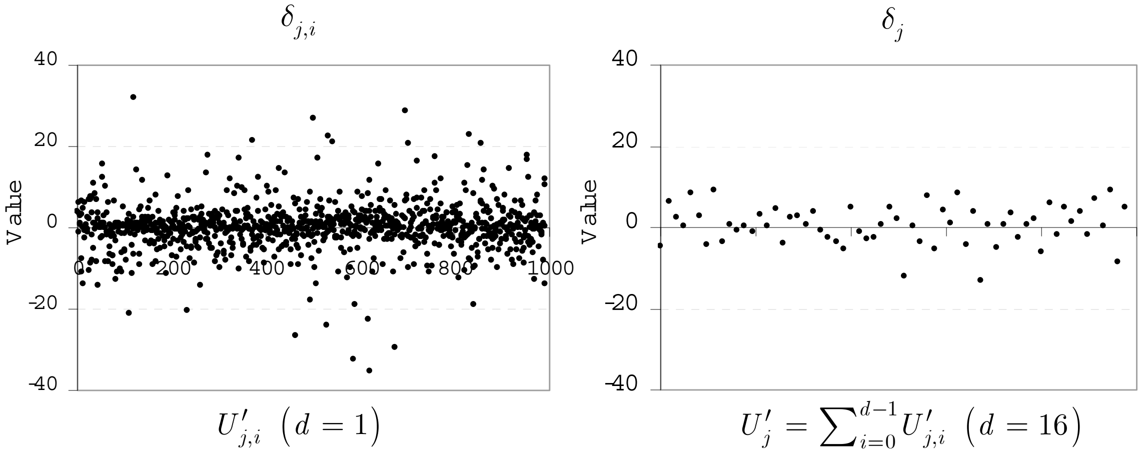


Figure 13. (**a**) The distribution of the ratio of the raw data level noise and Alice's CDF-transformed raw data units. It equals to 1 for a noise-free case; (**b**) The distribution of quantity $C\left(\Delta_{j,i}\right)/C\left(X_{j,i}\right)$.

In Figure 14a the distribution of noise $\delta_{j,i}$ on units $U'_{j,i}$ is shown, assuming that Bob selects $U_{j,i} \in \{-400/16, 400/16\}$.

In Figure 14b the distribution of δ_j on U'_j, using $U_j = \sum_{i=0}^{d-1} U_{j,i} \in \{-400, 400\}$ is depicted. The distribution of δ_j is given by the formula of $\mathbb{N}\left(0, \sigma_{\delta_j}^2\right)$, and the approximation of the binary Gaussian logical channel is justified by the CLT and the Lyapunov-condition.



(**a**) (**b**)

Figure 14. (**a**) The distribution of the unit-level noise $\delta_{j,i}$ on $U'_{j,i}$, $U_{j,i} \in \{-25, 25\}$, $\sigma_X^2 = 100$, $\sigma_{X'}^2 = 104$; (**b**) The noise $\delta_j = \sum_{i=0}^{d-1} \delta_{j,i} \in \mathbb{N}\left(0, \sigma_{\delta_j}^2\right)$ on $U'_j = \sum_{i=0}^{d-1} U'_{j,i}$ at $d = 16$. The precision of the physical-binary channel conversion gets closer to perfect as $d \to \infty$.

The results make it possible to achieve a high-precision conversion of the physical Gaussian quantum channel into a logical binary Gaussian channel. Precisely, only an approximation is possible by the logical layer manipulations, which gets closer to perfect as $d \to \infty$. At $d = 16$ the approximation is almost perfect, and the noise on $U'_j = \sum_{i=0}^{d-1} U'_{j,i}$ is a real Gaussian noise $\mathbb{N}\left(0, \sigma_{\delta_j}^2\right)$.

6. Conclusions

The CVQKD protocols are based on Gaussian modulation, and powerful post-processing is needed to maximize the extractable valuable information from the correlated raw data. The physical layer solutions for the reconciliation of Gaussian variables require tomography that is intractable in a practical CVQKD scenario. The reconciliation is also possible in the level of the logical layer by a classical authenticated communication channel, and by traditional algorithmical tools. The multidimensional approaches were developed for this purpose, however the use of complex multidimensional calculations is also not desirable in a practical scenario. The proposed scalar reconciliation eliminates the use of multidimensional spherical space along with the dimensional boundaries. The scalar reconciliation process neither requires any physical-layer tomography, and only standard operations and calculations needed in the level of raw data. The method provides an easy implementation to maximize the extractable valuable binary information from the correlated raw data to significantly boost up the key rates and to improve the distance ranges of CVQKD.

Supplementary Materials: Available online at www.mdpi.com/2076-3417/8/1/87/s1, Table S1: Summary of the notations.

Acknowledgments: This work was partially supported by the GOP-1.1.1-11-2012-0092 project sponsored by the EU and European Structural Fund, by the Hungarian Scientific Research Fund—OTKA K-112125, by the COST Action MP1006, and by the National Research Development and Innovation Office of Hungary (Project No. 2017-1.2.1-NKP-2017-00001).

Author Contributions: L.G. designed the protocol and wrote the manuscript. L.G. and S.I. analyzed the results. All authors reviewed the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **2008**, *4*, 726–730. [CrossRef]
2. Pirandola, S.; Garcia-Patron, R.; Braunstein, S.L.; Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **2009**, *102*, 050503. [CrossRef] [PubMed]
3. Pirandola, S.; Serafini, A.; Lloyd, S. Correlation matrices of two-mode bosonic systems. *Phys. Rev. A* **2009**, *79*, 052327. [CrossRef]
4. Pirandola, S.; Braunstein, S.L.; Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **2008**, *101*, 200504. [CrossRef] [PubMed]
5. Weedbrook, C.; Pirandola, S.; Lloyd, S.; Ralph, T. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **2010**, *105*, 110501. [CrossRef] [PubMed]
6. Weedbrook, C.; Pirandola, S.; Garcia-Patron, R.; Cerf, N.J.; Ralph, T.; Shapiro, J.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621. [CrossRef]
7. Sun, M.; Peng, X.; Shen, Y.; Guo, H. Security of a new two-way continuous-variable quantum key distribution protocol. *Int. J. Quant. Inf.* **2012**, *10*, 1250059. [CrossRef]
8. Sun, M.; Peng, X.; Guo, H. An improved two-way continuous-variable quantum key distribution protocol with added noise in homodyne detection. *J. Phys. B At. Mol. Opt. Phys.* **2013**, *46*, 085501. [CrossRef]
9. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **2011**, *84*, 062317. [CrossRef]
10. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E.; Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 032309. [CrossRef]
11. Leverrier, A.; Alleaume, R.; Boutros, J.; Zemor, G.; Grangier, P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A* **2008**, *77*, 042325. [CrossRef]
12. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2012**, *7*, 378–381. [CrossRef]
13. Leverrier, A.; Garcia-Patron, R.; Renner, R.; Cerf, N.J. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.* **2013**, *110*, 030502. [CrossRef] [PubMed]
14. Imre, S.; Gyongyosi, L. *Advanced Quantum Communications—An Engineering Approach*; Wiley-IEEE Press: Hoboken, NJ, USA, 2012.
15. Tse, D.; Viswanath, P. *Fundamentals of Wireless Communication*; Cambridge University Press: Cambridge, UK, 2005.
16. Hamkins, J.; Zeger, K. Asymptotically efficient spherical codes—Part I: Wrapped spherical codes. *IEEE Trans. Inform. Theory* **1997**, *43*, 1774–1785. [CrossRef]
17. Swaszek, P.F.; Thomas, B.J. Multidimensional spherical coordinates quantization. *IEEE Trans. Inform. Theory* **1983**, *29*, 570–576. [CrossRef]
18. Miller, K. *Multidimensional Gaussian Distributions*; Wiley: New York, NY, USA, 1964.
19. Hamkins, J. Design and Analysis of Spherical Codes. Ph.D. Dissertation, University Illinois at Urbana-Champaign, Champaign, IL, USA, 1996.
20. Conway, J.H.; Smith, D.A. *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*; A K Peters/CRC Press: Natick, MA, USA, 2003.
21. Richardson, T.; Urbanke, R. *Modern Coding Theory*; Cambridge University Press: New York, NY, USA, 2008.
22. Gersho, A. Asymptotically optimal block quantization. *IEEE Trans. Inform. Theory* **1979**, *25*, 373–380. [CrossRef]
23. Sakrison, D.J. A geometric treatment of the source encoding of a Gaussian random variable. *IEEE Trans. Inform. Theory* **1968**, *14*, 481–486. [CrossRef]
24. Hamkins, J.; Zeger, K. Gaussian source coding with spherical codes. *IEEE Trans. Inform. Theory* **2002**, *48*, 2980–2989. [CrossRef]
25. Hanzo, L.; Haas, H.; Imre, S.; O'Brien, D.; Rupp, M.; Gyongyosi, L. Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless. *Proc. IEEE* **2012**, *100*, 1853–1888. [CrossRef]
26. Rice, J.A. *Mathematical Statistics and Data Analysis*, 2nd ed.; Duxbury Press: Pacific Grove, CA, USA, 1995; ISBN 0-534-20934-3.

27. Botsinis, P.; Alanis, D.; Ng, X.S.; Hanzo, L. Low-Complexity soft-output quantum-assisted multi-user detection for direct-sequence spreading and slow subcarrier-hopping aided SDMA-OFDM systems. *IEEE Access* **2014**, *2*, 451–472. [CrossRef]
28. Botsinis, P.; Ng, S.X.; Hanzo, L. Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA. *IEEE Trans. Commun.* **2014**, *62*, 990–1000. [CrossRef]
29. Gyongyosi, L.; Imre, S. Geometrical analysis of physically allowed quantum cloning transformations for quantum cryptography. *Inf. Sci.* **2014**, *285*, 1–23. [CrossRef]
30. Gyongyosi, L.; Imre, S. Algorithmic superactivation of asymptotic quantum capacity of zero-capacity quantum channels. *Inf. Sci.* **2011**, *222*, 737–753. [CrossRef]
31. Gyongyosi, L.; Imre, S. Superactivation of quantum channels is limited by the quantum relative entropy function. *Quantum Inf. Process.* **2013**, *12*, 1011–1021. [CrossRef]
32. Gyongyosi, L.; Imre, S. Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution. In Proceedings of the Quantum Information and Computation XII, Baltimore, MD, USA, 22 May 2014. [CrossRef]
33. Imre, S.; Balazs, F. *Quantum Computing and Communications—An Engineering Approach*; John Wiley and Sons Ltd.: Hoboken, NJ, USA, 2005; ISBN 0-470-86902-X.
34. Petz, D. *Quantum Information Theory and Quantum Statistics*; Springer: Heidelberg, Germany, 2008.
35. Meter, R.V. *Quantum Networking*; John Wiley and Sons Ltd.: Hoboken, NJ, USA, 2014; ISBN 1118648927, 9781118648926.
36. Ruppert, L.; Usenko, V.C.; Filip, R. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Phys. Rev. A* **2014**, *90*, 062310. [CrossRef]
37. Lloyd, S. Capacity of the noisy quantum channel. *Phys. Rev. A* **1997**, *55*, 1613–1622. [CrossRef]
38. Renner, R.; Cirac, J.I. A de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **2009**, *102*, 110504. [CrossRef] [PubMed]
39. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **2012**, *109*, 100502. [CrossRef] [PubMed]
40. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501. [CrossRef] [PubMed]
41. Van Assche, G.; Cardinal, J.; Cerf, N.J. Reconciliation of a quantum-distributed Gaussian key. *IEEE Trans. Inf. Theory* **2004**, *50*, 394–400. [CrossRef]
42. Leverrier, A.; Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. *Phys. Rev. A* **2011**, *83*, 042312. [CrossRef]
43. Zwillinger, D.; Kokoska, S. *Standard Probability and Statistics Tables and Formulae*; CRC Press: Boca Raton, FL, USA, 2010; ISBN 978-1-58488-059-2.
44. Gentle, J.E. *Computational Statistics*; Springer: Berlin, Germany, 2009; ISBN 978-0-387-98145-1.
45. Billingsley, P. *Probability and Measure*, 3rd ed.; John Wiley & Sons: Hoboken, NJ, USA, 1995; ISBN 0-471-00710-2.
46. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2009**, *102*, 180504. [CrossRef] [PubMed]
47. Gyongyosi, L. Improved Long-Distance Two-way Continuous Variable Quantum Key Distribution over Optical Fiber. In Proceedings of the 2013 Frontiers in Optics/Laser Science XXIX (FiO/LS), Orlando, FL, USA, 6–10 October 2013.
48. Gyongyosi, L.; Imre, S. Long-distance continuous-variable quantum key distribution with advanced reconciliation of a Gaussian modulation. In Proceedings of the Advances in Photonics of Quantum Computing, Memory, and Communication VII, San Francisco, CA, USA, 19 February 2014; Volume 8997. [CrossRef]
49. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computer, Systems Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
50. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dusek, M.; Lutkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
51. Inoue, K.; Waks, E.; Yamamoto, Y. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A* **2003**, *68*, 022317. [CrossRef]

52. Stucki, D.; Brunner, N.; Gisin, N.; Scarani, V.; Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **2005**, *87*, 194108. [CrossRef]
53. Bacco, D.; Christensen, J.B.; Castaneda, M.A.U.; Ding, Y.; Forchhammer, S.; Rottwitt, K.; Oxenløwe, L.K. Two-dimensional distributed-phase-reference protocol for quantum key distribution. *Sci. Rep.* **2016**, *6*, 36756. [CrossRef] [PubMed]