Scalar Reconciliation for Gaussian Modulation of Two-Way Continuous-Variable Quantum Key Distribution

Laszlo Gyongyosi

1Quantum Technologies Laboratory, Department of Telecommunications
Budapest University of Technology and Economics
2 Magyar tudosok krt, Budapest, H-1117, Hungary
Information Systems Research Group, Mathematics and Natural Sciences
Hungarian Academy of Sciences
Budapest, H-1518, Hungary

gyongyosi@hit.bme.hu

Abstract

The two-way continuous-variable quantum key distribution (CVQKD) systems allow higher key rates and improved transmission distances over standard telecommunication networks in comparison to the one-way CVQKD protocols. To exploit the real potential of two-way CVQKD systems a robust reconciliation technique is needed. It is currently unavailable, which makes it impossible to reach the real performance of a two-way CVQKD system. 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 two-way 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 scalar space and the reconciliation can be extended to arbitrary high 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 two-way CVQKD. The proposed scalar reconciliation can also be applied in one-way systems as well, to replace the existing reconciliation schemes.

Keywords: continuous-variable quantum key distribution, reconciliation, Gaussian variables, Gaussian modulation, quantum cryptography, quantum Shannon theory.
1 Introduction

The QKD (Quantum Key Distribution) systems represent one of the most important practical applications of quantum information theory. The QKD schemes allow unconditionally secret communication between distant parties by exploiting the fundamental attributes of quantum mechanics. The QKD protocols can be classified into two main classes: DV (Discrete-Variable) and CV (Continuous-Variable) QKD 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 telecommunication networks and technologies that are currently available and in widespread use. As follows, the CVQKD systems can be integrated into the current telecommunication networks by using well-established optical fiber networks and practical devices. 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 the leak of only lower valuable information to the eavesdropper, and they are also equipped with significantly stronger capabilities in comparison to one-way protocols. Turning our attention to two-way CVQKD from one-way CVQKD is definitely reasonable, since one-way schemes have almost reached their physical limitations, and no significant further improvements can be realized in the secret key rates and transmission distances, neither by applying more robust post-processing nor by more powerful reconciliation techniques.

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, while the analysis of arbitrary attacks in the finite-size regime is currently in progress [9]. One of the most critical points in regard to CVQKD is the post-processing [1-11]. 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, generated by the random quadrature measurements at the parties. Each quadrature measurement results in a unit in the raw data. The raw data itself contains no 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. The logical-layer based post-processing 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 com-
mon 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, fortunately, 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. 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. [9-11]) 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 crucial role in CVQKD, since this phase makes it possible to correct the errors incurred on the quantum channel and to share an error-free key between Alice and Bob. Since the raw data is formulated by binary bitstrings 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. At this point we arrived 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.

Arrived to this point, we must declare explicitly what our main purposes are. 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, stronger than the one-way systems, 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 in eight. 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. As a fine corollary, 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, at this point one could recognize that, in fact, we do not have to decode the Gaussian variables in the multidimensional space. It is good news, since the arbitrary high-precision approximation of the logical binary Gaussian channel can be made in the non-spherical space by using considerable dimensions. This perception is definitely correct, however it is not trivial at first sight. We exploit it in this work to construct a scalar reconciliation that breaks with the traditions of the previously introduced multidimensional approaches [9-11], 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. Now, the question is straightforward. Is it possible to find such an efficient post-processing technique for the reconciliation of Gaussian variables without the need of physical-layer tomography and complex computations? The answer from now on is definitely, yes.

In this paper we define scalar reconciliation for CVQKD. We demonstrate the results for two-way CVQKD. The proposed method does the reconciliation of Gaussian variables without the need of any physical-layer tomography or multidimensional operations, and since the proposed scheme is backward compatible it also can be applied to one-way CVQKD. It brings significantly higher noise-resistance and information-transmission capability, extended transmission distances, and improved key rates.

This paper is organized as follows. In Section 2, the preliminary findings of two-way CVQKD are summarized. In Section 3, we introduce the proposed reconciliation scheme. Section 4 provides the theorems and proofs. In Section 5, the performance of the reconciliation scheme is studied. Finally, in Section 6, we conclude the paper. Supplemental information is included in the Appendix.

2 Two-Way Continuous-Variable QKD

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 \( N_1 \), 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 \( N_1 \). The reason for this is that the amount of valuable information transmitted over \( N_2 \) is already decreased by the attack of \( N_1 \). More attacks add more noise into the transmission, which also decreases the amount of mutual information between Alice and Bob. At this point one should ask, how we could gain any benefits from the decreased information that is contained in Bob’s received system. Or, why do we need a second channel use if it just adds more noise? The answer is so simple: Allow Eve to get as much less-valuable information as possible. We explicitly do this with the increased number of channel uses, because if Alice encodes her information into the noisy state that is received from \( N_1 \), and then sends it back to Bob over \( N_2 \), then the parties can achieve the desired phenomenon of superadditivity. So, the reason is now clear: the amount of valuable information leaked to Eve is also decreased by the multiple uses of the quantum channel. The price we have to pay is negligible, since 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 blindly attack the quantum channel. Thanks to her hot temperament, she will also simultaneously decrease the amount of eavesdropped information by her actions. And that is all we need to get higher key
rates in comparison to one-way CVQKD: to give lower valuable information to Eve. The idea works well, because in the post-processing phase the parties can correct the errors caused by Eve, so, 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 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 probably lower than between Alice and Eve [1-7, 9-14]. The reason: if Bob starts to run the reconciliation phase using the 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, that encodes her position and momentum quadratures and obtains a phase space vector $S_{Alice} = \ket{x_A + ip_A}$. Bob also draws a phase space vector $S_{Bob} = \ket{x_B + ip_B}$. 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:

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

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:

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

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 Fig. 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. Unfortunately, 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, denoted by $X'_j$. Bob then generates a random key $U_j$ (the full key vector $K$ is granulated into several $U_j$-s), and multiplies it with his raw data $C(X'_j)$. Alice receives $C(X'_j)U_j$, and using her $C(X_j)$, she computes the noisy $U'_j$. 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 $K$ between Alice and Bob. From Alice, it requires the correction of the noise on $U'_j$ to get back Bob’s $U_j$, using only scalar operations without the need of the multidimensional spherical space.

Fig. 1. The simplified view of a PM-RR two-way 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 $X' = M_2(\mathcal{N}_2(S_{Bob}(\mathcal{N}_1(S_{Bob}) + S_{Alice}))$.

In the next section, we discuss in detail the properties of the combined signal space and the effect of noise in the level of quadratures.
2.1 Direct coding in the combined phase space

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 $S_A$ by $x_{A,i}, p_{A,i}$, and the quadratures of Bob’s signal $S_{Bob,i}$ in the phase space $S_B$ by $x_{B,i}, p_{B,i}$, where $x_{A,i}, p_{A,i} \in \mathbb{N}(0, \sigma^2_\omega)$ and $x_{B,i}, p_{B,i} \in \mathbb{N}(0, \sigma^2_\omega)$ are drawn from a Gaussian random distribution with mean $\mu = 0$, and variance $\sigma^2_\omega$, where $\sigma^2_\omega$ is the modulation variance, which can be chosen to be equal to the shot noise at the parties [1-10]. The coherent states $\ket{x_{A,i}, p_{A,i}} \in S_A$ and $\ket{x_{B,i}, p_{B,i}} \in S_B$ are encoded by Gaussian modulation with dedicated centers $(x_{A,i}, p_{A,i}) \in S_A$ and $(x_{B,i}, p_{B,i}) \in S_B$, respectively. The two beams are correlated at Alice’s BS, which results in a combined signal in the combined phase space $S_{AxB}$. The modulation noise $\vartheta \in \mathbb{N}(0, 1)$, is precisely centered around $(x_{A,i} + x_{B,i}, p_{A,i} + p_{B,i}) \in S_{AxB}$ and $(x_{A,i} - x_{B,i}, p_{A,i} - p_{B,i}) \in S_{AxB}$ in $S_{AxB}$. 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 $M^i_1$ on the first mode of the beam, while the second mode is transmitted back to Bob over quantum channel $N_2$. Alice’s state in the combined phase space $S_{AxB}$ is as follows:

$$ \ket{\varphi_i} = \ket{x_{A,i} + x'_{B,i} + i(p_{A,i} + p'_{B,i})} \in \mathbb{N}(0, 2\sigma^2_\omega + \sigma^2_{N_1}) \in S_{AxB}, $$

(3)

where $2\sigma^2_\omega$ is the cumulated modulation variance, $\sigma^2_{N_1}$ is the variance of $N_1$, while $x'_{B,i}, p'_{B,i}$ are Bob’s noisy quadratures modified by $N_1$. Assuming a homodyne measurement $M^i_1$, 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:

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

(4)

or, if she used the momentum quadrature basis she gets

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

(5)

The second mode of the combined signal in $S_{AxB}$ is transmitted directly back to Bob over the noisy channel $N_2$, given as:

$$ \ket{\phi_i} = \ket{x_{A,i} - x'_{B,i} + i(p_{A,i} - p'_{B,i})} \in \mathbb{N}(0, 2\sigma^2_\omega + \sigma^2_{N_1}) \in S_{AxB}. $$

(6)

The Gaussian noise of the quantum channel $N_2$ defines a noise vector $\Delta_i \in \mathbb{N}(0, \sigma^2_{N_2}) \in S_{AxB}$, which results in the noisy state $\ket{\xi_i} \in S_{AxB}$ as follows:

$$ \ket{\xi_i} = \ket{\phi_i} + \Delta_i = \ket{x''_{A,i} - x''_{B,i} + i(p'_{A,i} - p''_{B,i})} \in \mathbb{N}(0, 2\sigma^2_\omega + \sigma^2_{N_1} + \sigma^2_{N_2}) \in S_{AxB}. $$

(7)

In the next phase, Bob applies a random quadrature measurement $M^i_2$ (assumed to be homodyne) and gets block $Y_i$. If he used a position quadrature basis, he gets
and for the momentum quadrature basis he obtains:

\[ Y'_i = p'_{A,i} - p''_{B,i}. \]  

(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:

\[ X'_i = Y'_i + 2x_{B,i} = x'_{A,i} - x''_{B,i} + 2x_{B,i} = x'_{A,i} + x''_{B,i}, \]  

(10)

and

\[ X'_i = Y'_i + 2p_{B,i} = p'_{A,i} - p''_{B,i} + 2p_{B,i} = p'_{A,i} + p''_{B,i}, \]  

(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 \( \Delta_i \) to Alice’s raw data block \( X_i \).

Alice’s and Bob’s modes in the combined phase space \( \mathcal{S}_{AxB} \) right after being outputted from the BS are \( |\varphi_i\rangle \) and \( |\phi_i\rangle \), as shown in Fig. 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 \( \mathcal{S}_{AxB} \) arises from the modulation noise \( \partial \in \mathbb{N}(0,1) \) (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 \( X'_i \in \mathbb{N}(0,\sigma'_X) \). The noise of the first channel changes the Gaussian random distribution \( \mathbb{N}(0,2\sigma^2_x) \) to \( \mathbb{N}(0,2\sigma^2_x + \sigma^2_{\mathcal{N}_1}) \) in the combined phase space \( \mathcal{S}_{AxB} \), with mean \( \mu = 0 \), and results \( X \) raw data level variance \( \sigma'^2_X = \left(2\sigma^2_x + \sigma^2_{\mathcal{N}_1}\right) \), and where noise variance \( \sigma^2_{\mathcal{N}_1} \) arises from the first channel use. The second mode of the coupled beam is also characterized by the same variance, i.e., \( |\phi_i\rangle \in \mathbb{N}(0,2\sigma^2_x + \sigma^2_{\mathcal{N}_1}) \). The noise of \( \mathcal{N}_2 \) transforms \( |\phi_i\rangle \in \mathcal{S}_{AxB} \) into \( |\xi_i\rangle \in \mathcal{S}_{AxB} \) and further modifies the distribution, so finally Bob’s received state will follow a Gaussian distribution \( \mathbb{N}(0,2\sigma^2_x + \sigma^2_{\mathcal{N}_1} + \sigma^2_{\mathcal{N}_2}) \). The \( X' \) raw data level variance is evaluated as \( \sigma'^2_{X'} = \left(2\sigma^2_x + \sigma^2_{\mathcal{N}_1} + \sigma^2_{\mathcal{N}_2}\right) \), which fact arises from the cumulated Gaussian random noise of \( \mathcal{N}_1 \) and \( \mathcal{N}_2 \). At this point, one can recognize that on the raw data level, only the difference of the variance of Alice’s and Bob’s raw data \( \sigma'^2_X \) and \( \sigma'^2_{X'} \) has relevance and \( \sigma'^2_{\mathcal{N}_1} \) vanishes from the picture. This difference is, indeed, \( \sigma'^2_{\mathcal{N}_2} \). 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 $2\sigma_w^2$ by $\sigma_{N_1}^2$, which finally results in $N\left(0,\sigma_x^2\right)$ on the level of raw data blocks. In particular only $N_2$ will have significance in the whole scenario, and, in fact, only the noise of the second channel use has to be corrected in the reconciliation phase.

$$S_{A\times B}$$

Fig. 2. The combined signals $\phi_i \in N\left(0,2\sigma_w^2 + \sigma_{N_1}^2\right)$ and $\phi_i \in N\left(0,2\sigma_w^2 + \sigma_{N_1}^2\right)$ in the combined phase space, $S_{A\times B}$. The modulation noise $\partial \in N\left(0,1\right)$ in the combined signal space $S_{A\times B}$ is illustrated by the Gaussian curves. The noise $\Delta_i \in N\left(0,\sigma_{N_2}^2\right)$ of quantum channel $N_2$ distorts $\phi_i \in N\left(0,2\sigma_w^2 + \sigma_{N_1}^2\right)$ into $\xi_i \in N\left(0,2\sigma_w^2 + \sigma_{N_1}^2 + \sigma_{N_2}^2\right)$. Alice’s raw data variance is $\sigma_x^2 = \left(2\sigma_w^2 + \sigma_{N_1}^2\right)$, while Bob’s raw data variance is $\sigma_{X'}^2 = \left(2\sigma_w^2 + \sigma_{N_1}^2 + \sigma_{N_2}^2\right)$.

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.

### 2.2 Uniform distribution in the multidimensional 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. What caused this? Let us reveal it.

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 $g \in N\left(0,1\right) \in \mathbb{R}$ is a real variable selected from a Gaussian distribution. A standard Gaussian variable $g \in N\left(0,1\right)$ 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 $g^* \in N\left(\mu,\sigma^2\right) \in \mathbb{R}$ with nonzero mean $\mu \neq 0$, and
variance $\sigma^2$, 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:

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

In Alice’s raw data, a $d$-dimensional Gaussian vector $\mathbf{X}_j = (X_{j,0}, \ldots, X_{j,d-1})^T \in \mathbb{N}(0, \sigma_X^2) \in \mathbb{R}^d$ 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 $\mathbb{N}(0, \sigma^2_X)$. Alice’s Gaussian vector is referred by $\mathbf{X}_j \in \mathbb{N}(0, \sigma_X^2) \in \mathbb{R}^d$, and its noisy version at Bob’s side is denoted by $\mathbf{X}'_j \in \mathbb{N}(0, \sigma_{X'}^2) \in \mathbb{R}^d$. 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 reason: the normalized $d$-dimensional Gaussian vectors change the probability distribution from Gaussian random to uniform on the $d$-dimensional unit sphere, $\Gamma^{d-1}$. Its relevance is clear at this point, since only uniform distribution is allowed in the reconciliation phase. Now, let us see what causes this property. 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 $\mathbf{X}'_j = (X'_{j,0}, \ldots, X'_{j,d-1})^T \in \mathbb{N}(0, \sigma_{X'}^2) \in \mathbb{R}^d$, where $X'_{j,i} \in \mathbb{N}(0, \sigma_{X'}^2) \in \mathbb{R}$, for $i \in [d]$. The $d$-length Gaussian random vector $\mathbf{X}'_j$ has norm $\|\mathbf{X}'_j\|$, mean $\mathbb{E}(\|\mathbf{X}'_j\|) = \sigma_{X'} \sqrt{d - \frac{1}{2}}$ and variance $\text{var}(\|\mathbf{X}'_j\|) \leq \frac{\sigma_{X'}^2}{2}$. We step further from this point. Since the variance of $\mathbf{X}'_j$ is not unit, the covariance matrix $\mathbf{C}(\mathbf{X}'_j)$ is not equal to identity, but the random units $X'_{j,i}$ are uncorrelated, so $\mathbf{C}(\mathbf{X}'_j)$ is diagonal. The normalized vector $\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}$, with norm $\|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|$, can be identified on the unit sphere $\Gamma^{d-1}$ [18,24], with radius $r = \|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|$. The mean of $\|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|$ is $\mathbb{E}(\|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|) = \sigma_{X'} \sqrt{d - \frac{1}{2}}/\sqrt{d\sigma_{X'}^2}$. The vector $\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}$ on the unit sphere $\Gamma^{d-1}$ is identified as $\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2} = r \frac{\mathbf{X}'_j}{\|\mathbf{X}'_j\|} = \frac{\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}}{\|\mathbf{X}'_j\|}\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}$. Precisely, the normalized quantity $\|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|$ has variance $\text{var}(\|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|) \leq \frac{\sigma_{X'}^2}{2}/\sqrt{d\sigma_{X'}^2}$.

From the spherical symmetry, it follows that if $d \to \infty$, the normalized random vector $\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}$ will be equipped with uniform distribution on $\Gamma^{d-1}$. The background of this phenomenon is as follows. First, for $d \to \infty$, the mean $\mathbb{E}[\cdot]$ of the normalized quantity $\|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|$ will tend to one, i.e., $\lim\limits_{d \to \infty} \mathbb{E}[\|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|] = \lim\limits_{d \to \infty} \frac{\sigma_{X'} \sqrt{d - \frac{1}{2}}}{\sqrt{d\sigma_{X'}^2}} = 1$. Second, the variance $\text{var}[\cdot]$ of $\|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|$ will tend to zero, $\lim\limits_{d \to \infty} \text{var}[\|\mathbf{X}'_j/\sqrt{d\sigma_{X'}^2}\|] = \lim\limits_{d \to \infty} \frac{\frac{\sigma_{X'}^2}{2}}{\sqrt{d\sigma_{X'}^2}} = 0$. These implies that
for $d \to \infty$, the normalized Gaussian random vector $X'_j / \sqrt{d\sigma^2_{X'}}$ becomes uniformly distributed on the unit sphere $\Gamma^{d-1}$. Third, as the dimension increases the distribution of the norm of $X'_j / \sqrt{d\sigma^2_{X'}}$ (i.e., the radius on $\Gamma^{d-1}$) will approximate the Dirac distribution $\mathcal{D}(d')$ [9-11,18], and it will also converge to one, $r = \lim_{d \to \infty} \left\| X'_j / \sqrt{d\sigma^2_{X'}} \right\| = 1$. The unit norms of $X'_j / \sqrt{d\sigma^2_{X'}}$ play exactly the role of unit fading-coefficients for a logical binary Gaussian channel, since during the transmissions of the messages generated from $X'_j / \sqrt{d\sigma^2_{X'}}$ the unit norms $r = \left\| X'_j / \sqrt{d\sigma^2_{X'}} \right\| = 1$ 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 $\mathcal{D}_d(x) = (1/a\sqrt{\pi})e^{-(x-a)^2/a^2}$, where $a = 1/\sqrt{d}$ and $r = \lim_{d \to \infty} \left\| X'_j \right\| = 1$.

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 $X'_j / \sqrt{d\sigma^2_{X'}}$ 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 (see next section). Analyzing the situation if the noisy raw data follows Gaussian random distribution with $\sigma^2_{X'} > 1$, the speed of convergence of the mean $\mathbb{E} \left[ X'_j / \sqrt{d\sigma^2_{X'}} \right]$ and variance $\text{var} \left[ X'_j / \sqrt{d\sigma^2_{X'}} \right]$ 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 $X'_j$ is summarized in Fig. 3.

![Fig. 3. The mean $\mathbb{E} [\cdot]$, variance $\text{var} [\cdot]$ of the normalized quantity $\left\| X'_j / \sqrt{d\sigma^2_{X'}} \right\|$ and the norm $\left\| X'_j / \sqrt{d\sigma^2_{X'}} \right\|$ of the normalized Gaussian random vector $X'_j / \sqrt{d\sigma^2_{X'}}$. Vector $X'_j$ 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.](image-url)
As we have mentioned, the multidimensional approaches are limited in $d = 8$ [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 $O_j \in \mathbb{R}^8$ is built up from eight units $X_{j,0...j,7} \in \mathbb{N}(0, \sigma_X^2)$, as:

$$O_j = X_{j,0} \text{Re} + X_{j,1} \text{Im}_1 + ... + X_{j,7} \text{Im}_7,$$

where $\text{Re} \in \mathbb{R}$ stands for the real part, while $\text{Im}_i \in \mathbb{C}$, for $i = 1,i \leq 7$ indentifies the $i$-th imaginary units, respectively. Bob’s noisy $O'_j$ is $O'_j = X'_{j,0} \text{Re} + X'_{j,1} \text{Im}_1 + ... + X'_{j,7} \text{Im}_7$, where $X'_{j,0...j,7} \in \mathbb{N}(0, \sigma_X^2)$. The octonions $O_j = \{X_{j,0}, X_{j,1},...,X_{j,7}\}$ and $O'_j = \{X'_{j,0}, X'_{j,1},...,X'_{j,7}\}$ are illustrated in Fig. 4. The Gaussian noise of the quantum channel distorts the elements $X_{j,i}$ of $O_j$, which represent the coefficients of the real and imaginary parts.

![Fig. 4. The raw data-level octonions $O_j$ and $O'_j$.](image)

To summarize, in the multidimensional case the uniformity of the $d$-dimensional Gaussian random raw data vectors $X_j \in \mathbb{R}^d$, $d \leq 8$, can be achieved only in the multidimensional spherical space, over the unit sphere $\Gamma^{d-1}$. 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 of the parties, which makes it possible to eliminate the spherical calculations from the reconciliation phase. First, let us see how scalar reconciliation changes this picture, what the motivations are, and what more adds to it.

### 3 Scalar 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 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 results in the $N$-unit length raw data vectors. Then formulate $N/d$ number of $d$-dimensional vectors $X_j \in \mathbb{R}^d$, $X'_j \in \mathbb{R}^d$. 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 $X_j \in \mathbb{R}^d$ and $X'_j \in \mathbb{R}^d$, for $j=0$, $j \leq (N/d) - 1$, of Alice and Bob are defined as:

$$X_j = \{X_{j,0},...,X_{j,d-1}\}^T \in \mathbb{N}(0, \sigma_X^2)$$

$$X'_j = \{X'_{j,0},...,X'_{j,d-1}\}^T \in \mathbb{N}(0, \sigma_X^2)$$
\[ X_j' = \left( X'_{j,0}, \ldots, X'_{j,d-1} \right)^T \in \mathbb{N}(0, \sigma^2_X), \]  
where \( X_{j,i} \in \mathbb{N}(0, \sigma^2_X) \) and \( X'_{j,i} \in \mathbb{N}(0, \sigma^2_X) \) 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 \( U_j \) is drawn from a uniform distribution \( \mathcal{U} \) and built up from \( d \) units, \( U_{j,i} \in \mathbb{R} \), as:

\[ U_j \in \mathbb{R}^d : \left( U_{j,0}, \ldots, U_{j,d-1} \right)^T, \quad U_{j,i} \in \mathbb{R}, \quad \text{for } j=0, j \leq \left( N/d \right) - 1. \]  
The \( d \) units \( U_{j,i} \in \mathcal{U} \) of \( U_j \) are uniform random variables, as follows:

\[ U_j \in \{a, b\} = \sum_{i=0}^{d-1} U_{j,i} \in \mathcal{U}. \]  

From (18) follows, that (17) can be rewritten as \( U_j \in \{a, b\} \subseteq \mathbb{R}^d \), with vectors \( \mathbf{A}, \mathbf{B} \) as:

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

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 \( K \) is built up as:

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

The reconciliation problem in the level of logical layer is summarized as follows. Alice and Bob first agree on \( d \). Bob sends the blocks of \( C(X'_j)U_j \in \mathbb{R}^d \), for \( j=0, j \leq \left( N/d \right) - 1 \), over the classical channel. Alice then receives the \( d \) noisy \( U'_{j,i} \) units, and by using her X she has to decode \( U'_j \) as \( \sum_{i=0}^{d-1} U'_{j,i} = \left( \sum_{i=0}^{d-1} C(X'_{j,i}) \right) \sum_{i=0}^{d-1} C(X_{j,i}) \sum_{i=0}^{d-1} U_{j,i} \) [9] and then she has to make an error-correction to remove the noise from \( U'_j \).

### 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 uniformity of the correlated raw data units is achieved by the Gaussian Cumulative Distribution Function (CDF). Another important difference is that the approximation of the logical binary Gaussian channel can be achieved by arbitrary dimensional vectors with arbitrary accuracy, which is justified by the Central Limit Theorem (CLT).
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 \( \mathcal{N}(0, \sigma_X^2) \). The Gaussian CDF-transformation \( C(\cdot) : \mathbb{R} \rightarrow \mathbb{R} \) for a unit \( X_{j,i}' \) is as follows:

\[
C(X_{j,i}') = \frac{1}{2} \left( 1 + \text{erf} \left( \frac{X_{j,i}'}{\sqrt{2} \sigma_X} \right) \right), \quad \text{for } i \in [d], \tag{21}
\]

where \( \text{erf} \left( \frac{X_{j,i}'}{\sqrt{2} \sigma_X} \right) = \frac{2}{\sqrt{\pi}} \int_0^{X_{j,i}'} e^{-t^2} \, dt \) is the Gauss error function, and \( C(X_{j,i}') \in \mathbb{R} \) is a real variable from the range of \([0,1]\), with \( \mathcal{U} \) uniform distribution (for a plausible example see Supplementary Information). The quantity \( C(X_{j,i}') \) will be referred as the CDF-transformed unit.

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

\[
C(X_{j,i}) = \frac{1}{2} \left( 1 + \text{erf} \left( \frac{X_{j,i}}{\sqrt{2} \sigma_X} \right) \right), \quad \text{for } i \in [d], \tag{22}
\]

and the result of (21) and (22) is the correlated uniform raw data \( C(X_{j,i}) \approx C(X_{j,i}') \). In the reconciliation process, only Alice can correct \( U_j' \) into \( U_j \), because nobody knows the CDF-transformed raw data units \( C(X_{j,i}) \), except Alice.

For a given \( X_j \in \mathbb{R}^d \), the CDF function \( C(\cdot) : \mathbb{R} \rightarrow \mathbb{R} \) reads as

\[
C(X_j) = C(X_{j,0}), \ldots, C(X_{j,d-1}) = \frac{1}{2} \left( 1 + \text{erf} \left( \frac{X_{j,i}}{\sqrt{2} \sigma_X} \right) \right) \in \mathbb{R}, \quad \text{for } i \in [d], \tag{23}
\]

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

\[
C(X_j') = C(X_{j,0}'), \ldots, C(X_{j,d-1}') = \frac{1}{2} \left( 1 + \text{erf} \left( \frac{X_{j,i}'}{\sqrt{2} \sigma_X} \right) \right) \in \mathbb{R}, \quad \text{for } i \in [d]. \tag{24}
\]

The CDF-transformed \( C(X_j) \), \( C(X_j') \) raw data vectors each consist of \( d \) real \( \mathbb{R} \) variables as:

\[
C(X_j) = \bigcup_{i=0}^{d-1} C(X_{j,i}), \quad C(X_j') = \bigcup_{i=0}^{d-1} C(X_{j,i}'). \tag{25}
\]

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 and a mathematical result from the 19th century – the so-called Lyapunov-condition [26]. 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 coincides 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 $U_j = \left(U_{j,0}, \ldots, U_{j,d-1}\right)^T$, 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 $\mathbb{E}[\delta_{j,i}] = \mu_{\delta_{j,i}} = 0$, noise variance $\text{var}[\delta_{j,i}] = \sigma_{\delta_{j,i}}^2$ (see Section 3.1 and 3.3 for a detailed derivation) as follows:

$$CLT:\quad \frac{1}{\sqrt{\sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2}} \delta_j = \frac{1}{\sqrt{\sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2}} \left(\sum_{i=0}^{d-1} \delta_{j,i}\right) \to \mathbb{N}\left(0, 1\right)_d$$

$$\delta_j = \left(\sum_{i=0}^{d-1} \delta_{j,i}\right) \to \mathbb{N}\left(0, \sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2\right) = \mathbb{N}\left(0, \sigma_{\delta_{j,d}}^2\right)$$

(26)

To show that (26) holds for the $d$-dimensional noise parameter $\delta_j$, we exploit the Lyapunov-condition [26]. Let $\mathcal{L} > 0$, then

$$\lim_{d \to \infty} \frac{1}{\sqrt{\sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2}} \sum_{i=0}^{d-1} \mathbb{E}\left[|\delta_{j,i}|^{2+2}\right] = 0$$

(27)

is satisfied for any $d \to \infty$, by theory. As follows, the noise on $U_j \in \mathbb{R}^d$ will converge to $\delta_j = \left(\sum_{i=0}^{d-1} \delta_{j,i}\right) \in \mathbb{N}\left(0, \sigma_{\delta_{j,d}}^2\right)$, and the resulting logical channel will be equivalent to a logical binary Gaussian channel with noise variance $\sigma_{\delta_{j,d}}^2$. By the same argumentation, the variance of the resulting logical binary Gaussian channel will converge to the variance of the physical Gaussian quantum channel $\sigma_{\mathcal{N}_2}^2$ for $N \to \infty$.

Let again $\mathcal{L} > 0$, and $d$ is an appropriate dimension for which (27) is satisfied, and let the expected variance of $\delta_j$ is $\text{var}[\delta_{j,i}] = \sigma_{\delta_{j,d}}^2$. Then

$$\lim_{N \to \infty} \frac{1}{\sqrt{\sum_{j=0}^{N/d-1} \sigma_{\delta_{j}}^2}} \sum_{j=0}^{N/d-1} \mathbb{E}\left[|\delta_{j}|^{2+2}\right] = 0$$

(28)

is satisfied by theory, from which

$$CLT:\quad \frac{1}{\sqrt{\sum_{j=0}^{N/d-1} \sigma_{\delta_{j}}^2}} \left(\sum_{j=0}^{N/d-1} \delta_j\right) \to \mathbb{N}\left(0, 1\right)_{N/d}$$

$$\left(\sum_{j=0}^{N/d-1} \delta_j\right) \to \mathbb{N}\left(0, \sum_{j=0}^{N/d-1} \sigma_{\delta_{j,d}}^2\right) = \mathbb{N}\left(0, \sigma_{\mathcal{N}_2}^2\right)_{N/d}$$

(29)

follows, which proves the statement.

Hence one can readily recognize that $\lim_{N \to \infty} \text{var}[\delta_{0\ldots(N/d)-1}] = \left(\sigma_{\mathcal{N}_2}^2\right)_{N/d}$. To conclude the situation, in (26) and (29) the variances of $\delta_j$ 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 bi-

16
nary Gaussian channel with noise variance $d\sigma^2_{\delta_j} \approx \sigma^2_{\mathcal{N}_2}$ for arbitrary $d$. In other words, 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, because the noise variance $\sigma^2_{\delta_j}$ is lower bounded by $\sigma^2_{\mathcal{N}_2}$, i.e.,

$$\sigma^2_{\delta_j} \geq \sigma^2_{\mathcal{N}_2}$$

holds, 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 which 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.

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 $\Gamma^{d-1}$ of $\mathbb{R}^d$ into $\mathbb{R}$. At this point, the main drawback of the multidimensional reconciliation approaches has to be clear: the processes required the use of spherical space $\Gamma^{d-1}$ 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. Why? Because, the fact, that the uniformly distributed elements of $\mathbb{R}^d$ have to be transmitted over the classical authenticated channel, 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 $\Gamma^{d-1}$ 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 $\mathbb{R}$.

At this point, 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 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 $n \equiv N/d$ number of $d$-dimensional vectors $X_j' = \left( X_{j,0}', \ldots, X_{j,d-1}' \right)^T \in \mathbb{R}^d$, where $d$ is the length of the vectors measured in units $X_{j,i}'$ in the raw data. Then for each $X_j'$, applies CDF transformation $C$ on the units $X_{j,i}' \in \mathbb{R}$ of $X_j'$, for $i = 0, i \leq d - 1$, for $j = 0, j \leq \left( N/d \right) - 1$. Bob generates $U_j = \left( U_{j,0}, \ldots, U_{j,d-1} \right)^T \in \mathbb{R}^d$, $U_{j,i} \in \mathbb{R}$, computes $C(X_j')U_j$, and sends it to Alice over the classical authenticated channel. Alice also divides her $N$-unit length raw data $X_j$, into $n \equiv N/d$ number of $d$-dimensional vectors $X_j = \left( X_{j,0}, \ldots, X_{j,d-1} \right)^T \in \mathbb{R}^d$, computes the CDF-transformed vectors $C(X_j)$ and decodes as $U_j' = C(X_j')U_j \frac{1}{C(X_j)} = \sum_{i=0}^{d-1} U_{j,i} = \frac{\sum_{i=0}^{d-1} C(X_{j,i})}{\sum_{i=0}^{d-1} C(X_{j,i})} \sum_{i=0}^{d-1} U_{j,i}$. Next, she corrects the Gaussian noise on $U_j'$ to get $U_j$. From these she rebuilds the error-free full key $K \in \mathbb{R}^{N/d} : \left( U_0, \ldots, U_{(N/d)-1} \right)^T$.

### 3.4 Security of scalar reconciliation

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 $C(X_j')U_j$ messages follow uniform distribution, and the multiplied $U_j$ and $X_j'$ vectors are also uniform and independent. The following conditional probability holds for each $U_j$:

$$\Pr\left( U_j = U_{0\ldots1} \middle| C(X_j')U_j \right) = \frac{1}{2}. \tag{30}$$

Since $C(X_j')U_j$ are uniformly distributed, and also independent [11], it follows that:

$$\Pr\left( C(X_{j,i}) = C(X_{j,0}) \ldots C(X_{j,N-1}) \right) = \frac{1}{N} \tag{31}$$

and

$$\Pr\left( U_j = U_{0\ldots1} \right) = \frac{1}{2}. \tag{32}$$

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

$$\Pr_{Eve}\left( K = \left( U_0, \ldots, U_{(N/d)-1} \right)^T \right) = \frac{1}{2^{N/d}}. \tag{33}$$

### 3.5 Noise on the raw data and the secret key

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 into consideration in the error correction.
The \(d\)-dimensional noise vector \(\Delta_j \in \mathbb{N}\left(0, \sigma_{N_2}^2\right)\) of the Gaussian channel \(N_2\) on the \(j\)-th \(X'_j\) is a Gaussian random vector defined as:

\[
\Delta_j = X'_j - X_j = \{\Delta_{j,0}, \ldots, \Delta_{j,d-1}\} \in \mathbb{N}\left(0, \sigma_{N_2}^2\right) \in \mathbb{R}^d,
\]

where \(\Delta_{j,i} \in \mathbb{N}\left(0, \sigma_{N_2}^2\right) \in \mathbb{R}\) identifies the Gaussian noise on the \(i\)-th unit \(X_i\) of \(X'_j\) as:

\[
\Delta_{j,i} = X'_{j,i} - X_{j,i} \in \mathbb{N}\left(0, \sigma_{N_2}^2\right) \in \mathbb{R}.
\]

The noise vector \(\Delta_j\) is added to Alice’s \(X_j\), hence Bob’s noisy \(X'_j\) is:

\[
X'_j = X_j + \Delta_j \in \mathbb{R}^d.
\]

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

\[
X'_{j,i} = X_{j,i} + \Delta_{j,i} \in \mathbb{R},
\]

and (36) can be rewritten as:

\[
X'_j = \{X'_{j,0}, \ldots, X'_{j,d-1}\} = \{X_{j,0} + \Delta_{j,0}, \ldots, X_{j,d-1} + \Delta_{j,d-1}\}.
\]

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 \(C\left(X'_j\right)U_j\) from Bob, from which she obtains \(\sum_{i=0}^{d-1} C\left(X'_{j,i}\right)\sum_{i=0}^{d-1} U_{j,i}\) and divides it by her \(\sum_{i=0}^{d-1} C\left(X_{j,i}\right)\). The effect of Gaussian noise \([9]\) results in a distorted secret \(U'_j \in \mathbb{R}\) as:

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

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

\[
\delta_{j,i} = \frac{U_{j,i}}{C(X_{j,i})} C\left(\Delta_{j,i}\right) \in \mathbb{N}\left(0, \sigma_{\delta_{j,i}}^2\right),
\]

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

\[
C\left(\Delta_{j,i}\right) = C\left(X'_{j,i}\right) - C\left(X_{j,i}\right) \in \mathbb{R},
\]

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

\[
U_j = \sum_{i=0}^{d-1} U'_{j,i} - \sum_{i=0}^{d-1} \delta_{j,i} = U_j - \zeta_j \in \mathbb{R},
\]
where $\varsigma_{j,i} \in \mathbb{N}\left(0, \sigma^2_{\varsigma_{j,i}}\right)$ characterizes the same amount of noise as (40), i.e., and $\varsigma_{j,i} = \delta_{j,i}$, however it is evaluated from the noisy raw-data units $U'_{j,i}$, $C\left(X'_{j,i}\right)$ as:

$$\varsigma_{j,i} = \frac{U_{j,i}}{C(\Delta_{j,i})} C\left(X'_{j,i}\right) \in \mathbb{R}, \quad (43)$$

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

$$U'_j = U_j + \delta_j \in \mathbb{R}^d, \quad (44)$$

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

$$\delta_j = \frac{U_j}{C(X_j)} C(\Delta_j) \in \mathbb{N}\left(0, \sigma^2_{\delta_j}\right) = \mathbb{N}\left(0, \bigcup_{i=0}^{d-1} \sigma^2_{\delta_{j,i}}\right). \quad (45)$$

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

$$\delta_j = \sum_{i=0}^{d-1} \delta_{j,i} = \frac{\sum_{i=0}^{d-1} C(\Delta_{j,i}) \sum_{i=0}^{d-1} U_{j,i}}{\sum_{i=0}^{d-1} C(X_{j,i})} \in \mathbb{N}\left(0, \sigma^2_{\delta_j}\right) = \mathbb{N}\left(0, \bigcup_{i=0}^{d-1} \sigma^2_{\delta_{j,i}}\right). \quad (46)$$

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

$$U_j = U'_j - \zeta_j \in \mathbb{R}^d, \quad (47)$$

and the noise vector $\zeta_j = \{\zeta_{j,0}, \ldots, \zeta_{j,d-1}\} \in \mathbb{R}^d$ is as follows:

$$\zeta_j = \frac{U'_j}{C(X'_j) + C(\Delta_j)} C(\Delta_j) \in \mathbb{N}\left(0, \sigma^2_{\zeta_j}\right) = \mathbb{N}\left(0, \bigcup_{i=0}^{d-1} \sigma^2_{\zeta_{j,i}}\right). \quad (48)$$

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

$$\varsigma_j = \sum_{i=0}^{d-1} \varsigma_{j,i} = \frac{\sum_{i=0}^{d-1} C(\Delta_{j,i}) \sum_{i=0}^{d-1} U'_{j,i}}{\sum_{i=0}^{d-1} C(X'_{j,i})} \in \mathbb{N}\left(0, \sigma^2_{\varsigma_j}\right) = \mathbb{N}\left(0, \bigcup_{i=0}^{d-1} \sigma^2_{\varsigma_{j,i}}\right). \quad (49)$$

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 $\Delta_{j,i} \in \mathbb{N}\left(0, \sigma^2_{X'_{j,i}}\right)$. In Fig. 5, the difference of the raw data-level units $X_{j,i}$ and $X'_{j,i}$ of $X_j$ and $X'_j$ are shown, where $\Delta_{j,i}$ is the noise vector of $\mathcal{N}_{2}$. Bob’s secret key unit is depicted by $U_{j,i}$, $U'_{j,i}$ is Alice’s received noisy key unit, while $\delta_{j,i} = \frac{U_{j,i}}{C(X_{j,i})} C(\Delta_{j,i})$ is the noise on a secret unit $U'_{j,i}$.
The difference of the units $X_{j,i}$ and $X'_{j,i}$ identifies a unit $\Delta_{j,i}$ from the noise vector $\Delta_j$ of $\mathcal{N}_2$. The difference of secret key units $U_{j,i}$ and $U'_{j,i}$ is $\delta_{j,i}$.

To step further, at this point we have to analyze in detail the properties of the noise vector $\Delta_{j,i}$. The noise vector $\Delta_j \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_2}\right) \in \mathbb{R}^d$ of $\mathcal{N}_2$ that generates the noisy $X'_j$ from $X_j$ is characterized as follows. First we decompose the noise vector $\Delta_j$ into its components:

$$\Delta_j = A_j \Lambda_j,$$

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

$$f(\Lambda_j) = \frac{1}{(2\pi)^{d/2}} e^{-\frac{\|\Lambda\|^2}{2}},$$

where $\|\Lambda\| = \sqrt{\Lambda_{j,0}^2 + \ldots + \Lambda_{j,d-1}^2}$ 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:

$$f(\Delta_j) = \frac{1}{(2\pi)^{d/2} \det A_j A_j^T} e^{-\frac{1}{2} \Delta_j^T (A_j A_j^T)^{-1} \Delta_j},$$

where $A_j A_j^T$ stands for the $\mathcal{C}(\Delta_j)$ covariance matrix of $\Delta_j$, and it analogous of $\sigma^2_{\mathcal{N}_2}$, i.e., in a more precise form $\mathcal{C}(\Delta_j) = \mathbb{E}(\Delta_j \Delta_j^T) = A_j A_j^T$. The noise on the units $X'_{j,i}$ of $X'_j$ 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 $\Delta_j \in \mathbb{N}(0,\sigma^2_{\mathcal{N}_2})_d$ is built up by $d$ components, $\Lambda_{j,i} \in \mathbb{N}(0,1) \in \mathbb{R}$ and $\Delta_{j,i} \in \mathbb{N}(0,\sigma^2_{\mathcal{N}_2}) \in \mathbb{R}$. The error $\Delta_{j,i}$ on the $i$-th unit $X'_{j,i}$ is as follows:

$$\Delta_{j,i} = A_{j,i} \Lambda_{j,i}, \text{ for } i = 0, i \leq d - 1,$$
where $A_{j,i}$ is a linear transformation that scales $\Lambda_{j,i}$. The probability density function of $\Lambda_{j,i}$ is:

$$f(\Lambda_{j,i}) = \frac{1}{\sqrt{2\pi}} e^{-\frac{\|\Lambda_{j,i}\|^2}{2}},$$  \hspace{1cm} (54)

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:

$$f(\Delta_{j,i}) = \frac{1}{\sqrt{2\pi} \sqrt{\det A_{j,i}^T A_{j,i}}} e^{-\frac{1}{2} \Delta_{j,i}^T (A_{j,i}^T)^{-1} \Delta_{j,i}},$$  \hspace{1cm} (55)

where $A_{j,i} A_{j,i}^T = E(\Delta_{j,i} \Delta_{j,i}^T) = C(\Delta_{j,i})$. From $\Lambda_{j,i}$ and $\Delta_{j,i}$, the correction of Bob’s noisy secret $U_j$ can be approached by the units $\{U'_{j,0}, \ldots, U'_{j,d-1}\}$, 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 (40).

Let us denote by $[\phi_{j,i}]$ the phase-space representation of Alice’s noise-free raw data unit $X_{j,i}$ given by (6), and by $[\xi_{j,i}]$ the noisy raw data unit $X'_{j,i}$ of Bob, from (7). (State $[\phi_{j,i}]$ is the second mode of the combined beam, while $[\xi_{j,i}]$ is its noisy version). The impact of $\Lambda_{j,i}$ on $[\phi_{j,i}]$ in $\mathcal{S}_{AxB}$ is depicted in Fig. 6. The $x$ and $p$ quadratures of $[\phi_{j,i}] \in \mathcal{S}_{AxB}$ are modified by $\Lambda_x$ and $\Lambda_p$ in the noisy $[\xi_{j,i}] \in \mathcal{S}_{AxB}$.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig6.png}
\caption{Assuming a standard Gaussian random noise on the quantum channel $\mathcal{N}_2$, a rotation is caused in the combined phase space $\mathcal{S}_{AxB}$ ($x$: position quadrature, $p$: momentum quadrature). The initial state $[\phi_{j,i}]$ is transformed into $[\xi_{j,i}]$. The magnitude $\|\Lambda_{j,i}\|$ of $\Lambda_{j,i} \in \mathbb{N}(0,1)$ is preserved in each direction, and follows a circular symmetry as depicted by the circles.

The effect of the real Gaussian noise of the quantum channel is shown in Fig. 7. The noise vector $\Delta_{j,i} \in \mathbb{N}(0, \sigma_{\mathcal{N}_2}^2) \in \mathcal{S}_{AxB}$ 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 $A_{j,i}$ resulting in ellipses. The magnitude $\|\Delta_{j,i}\|$ of $\Delta_{j,i}$ is not preserved in all directions, which leads to different density. The $x$ and $p$ quadratures of $[\phi_{j,i}] \in \mathcal{S}_{AxB}$ are modified by $\Delta_x$ and $\Delta_p$ in $[\xi_{j,i}] \in \mathcal{S}_{AxB}$.}
\end{figure}
Fig. 7. The real Gaussian noise of the quantum channel $\mathcal{N}_2$ causes a rotation and rescaled vector in the combined phase space $S_{A \times B}$ ($x$: position quadrature, $p$: momentum quadrature). The magnitude $||\Delta_{j,i}||$ of the noise vector $\Delta_{j,i} \in \mathbb{N}(0,\sigma^2_{\mathcal{N}_2})$ is not preserved, since the noise characteristic describes an ellipse in the combined phase space.

Next we show that reconciliation process of noisy Gaussian vectors can be restricted to operations in the scalar space, as Section 4 will reveal.

4 Theorems and Proofs

First we show that Alice’s noisy secret can be corrected in the 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 $\Gamma^{d-1}$.

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

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

$$U_j = A : ||U_j' - A|| < ||U_j' - B||,$$

$$U_j = B : ||U_j' - A|| > ||U_j' - B||.$$
where the quantity \( \| \mathbf{U}_j' - \mathbf{U}_j \| \), \( \mathbf{U}_j \in \{ \mathbf{A}, \mathbf{B} \} \) is evaluated as

\[
\| \mathbf{U}_j' - \mathbf{U}_j \| = \sqrt{\sum_{i=0}^{d-1} \left( \mathbf{U}_{j,i}' - \mathbf{U}_{j,i} \right)^2} = \sqrt{\sum_{i=0}^{d-1} \left( \frac{U_{j,i}}{C(X_{j,i})} C(\Delta_{j,i}) \right)^2} = \sqrt{\sum_{i=0}^{d-1} \left( \delta_{j,i} \right)^2} = \| \delta_j \|,
\]

which precisely coincidences with the norm of the Gaussian noise in (46). However, since Alice does not know Bob’s \( U_{j,i} \), in (58) an additional noise, \( \Upsilon_j \), also brings up, i.e., \( \| \mathbf{U}_j' - \mathbf{U}_j \| = \| \delta_j + \Upsilon_j \| \). The noise vector \( \Upsilon_j \) with expected variance \( \sigma_{\Upsilon_j}^2 \) 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 \( \mathbf{U}_j' \in \{ \mathbf{U}_j', \ldots, \mathbf{U}_{j,d-1}' \} \in \mathbb{R}^d \), and corrects \( \mathbf{U}_j' \) into \( \mathbf{U}_j \) and then from the components she rebuilds the full key \( \mathbf{K} = \left( \mathbf{U}_0, \ldots, \mathbf{U}_{(N/d)-1} \right)^T \in \mathbb{R}^{N/d} \). The error-vector \( \tilde{\delta}_j \in \mathbb{R}^d \) on a given noisy \( \mathbf{U}_j' \) is

\[
\tilde{\delta}_j = \sum_{i=0}^{d-1} \delta_{j,i} = \left( \frac{U_{j,i}}{C(X_{j,i})} \right)^T C(\Delta_{j,i}) \in \mathbb{N} \left\{ 0, \sigma_{\delta_j}^2 = \mathbb{E} \left( \left( \frac{U_{j,i}}{C(X_{j,i})} \right)^T C(\Delta_{j,i}) \right) \right\}_d
\]

(59)

The covariance matrix of (59) is expressed as:

\[
\mathbb{E} \left( \left( \frac{U_{j,i}}{C(X_{j,i})} \right)^T C(\Delta_{j,i}) \right) = \mathbb{E} \left( \left( \frac{U_{j,i}}{C(X_{j,i})} \right)^T C(\Delta_{j,i}) \right)^T \left( \frac{U_{j,i}}{C(X_{j,i})} \right) \right) \right) = \left( \sigma_{\delta_j}^2 \right)_d
\]

(60)

along with

\[
\delta_{j,i} = \left( \frac{U_{j,i}}{C(X_{j,i})} \right)^T C(\Delta_{j,i}) \in \mathbb{N} \left\{ 0, \sigma_{\delta_j}^2 = \mathbb{E} \left( \left( \frac{U_{j,i}}{C(X_{j,i})} \right)^T C(\Delta_{j,i}) \right) \right\}_d \in \mathbb{R},
\]

(61)

and (61) is characterized by covariance matrix

\[
\mathbb{E} \left( \left( \frac{U_{j,i}}{C(X_{j,i})} \right)^T C(\Delta_{j,i}) \right) = \mathbb{E} \left( \left( \frac{U_{j,i}}{C(X_{j,i})} \right)^T C(\Delta_{j,i}) \right)^T \left( \frac{U_{j,i}}{C(X_{j,i})} \right) \right) = \sigma_{\delta_j}^2.
\]

(62)

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

\[
\mathbf{U}_j = \mathbf{U}_j' - \tilde{\xi}_j \in \mathbb{R}^d,
\]

(63)

where

\[
\tilde{\xi}_j = \left( \frac{U_{j,i}'}{C(X_{j,i})+C(\Delta_{j,i})} \right)^T C(\Delta_j) \in \mathbb{N} \left\{ 0, \sigma_{\tilde{\xi}_j}^2 = \mathbb{E} \left( \left( \frac{U_{j,i}'}{C(X_{j,i})+C(\Delta_{j,i})} \right)^T C(\Delta_j) \right) \right\}_d
\]

\[
\mathbb{E} \left( \left( \frac{U_{j,i}'}{C(X_{j,i})+C(\Delta_{j,i})} \right)^T C(\Delta_{j,i}) \right) = \mathbb{E} \left( \left( \frac{U_{j,i}'}{C(X_{j,i})+C(\Delta_{j,i})} \right)^T C(\Delta_{j,i}) \right)^T \left( \frac{U_{j,i}'}{C(X_{j,i})+C(\Delta_{j,i})} \right) \right) = \sigma_{\tilde{\xi}_j}^2.
\]

(64)

The covariance matrix of (64) is as follows:
\[
\mathcal{E}\left(\left(\frac{U_j}{C(x_j + C(\Delta_j))}\right)^T C(\Delta_j)\right) = \mathbb{E}\left(\left(\frac{U_j}{C(x_j + C(\Delta_j))}\right)^T C(\Delta_j)\right) = \left(\sigma^2_{\delta_j}\right)_d \quad (65)
\]
and
\[
\varsigma_{j,i} = \frac{U_{j,i}}{C(x_{j,i} + C(\Delta_{j,i}))} C(\Delta_{j,i}) \in \mathbb{N}\left(0, \sigma^2_{\varsigma_{j,i}} = \mathcal{E}\left(\frac{U_{j,i}}{C(x_{j,i} + C(\Delta_{j,i}))} C(\Delta_{j,i})\right)\right), \quad (66)
\]
along with
\[
\mathcal{E}\left(\frac{U_{j,i}}{C(x_{j,i} + C(\Delta_{j,i}))} C(\Delta_{j,i})\right) = \mathbb{E}\left(\frac{U_{j,i}}{C(x_{j,i} + C(\Delta_{j,i}))} C(\Delta_{j,i})\right) = \left(\sigma^2_{\varsigma_{j,i}}\right). \quad (67)
\]
From (61) and (66) the quantities \(U_{j,i}\) and \(U'_{j,i}\) are evaluated as follows:
\[
U_{j,i} = U'_{j,i} - \frac{U'_{j,i}}{C(x_{j,i})} C(\Delta_{j,i}) = U'_{j,i} - \varsigma_{j,i} \in \mathbb{R}, \quad (68)
\]
and
\[
U'_{j,i} = \frac{C(x_{j,i})}{C(x_{j,i})} U_{j,i} = U_{j,i} + \delta_{j,i} \in \mathbb{R}. \quad (69)
\]
Let us denote by \(\nu\) the standard deviation of \(\tilde{\delta}_j + \tilde{\Upsilon}_j = \sum_{i=0}^{d-1} \delta_{j,i} + \sum_{i=0}^{d-1} \Upsilon_{j,i}\), which is evaluated from (65) and \(\sigma^2_{\Upsilon_j}\) as
\[
\nu = \sqrt{\left(\sigma^2_{\delta_j} + \sigma^2_{\Upsilon_j}\right)}_d. \quad (70)
\]
The maximum-likelihood-based correction rules can be given in the form of:
\[
U_j = A : \frac{1}{\left(\pi 2\nu^2\right)^{d/2}} e^{-\frac{\|U_j-A\|^2}{2\nu^2}} \geq \frac{1}{\left(\pi 2\nu^2\right)^{d/2}} e^{-\frac{\|U_j-B\|^2}{2\nu^2}}, \quad (71)
\]
and:
\[
U_j = B : \frac{1}{\left(\pi 2\nu^2\right)^{d/2}} e^{-\frac{\|U_j-A\|^2}{2\nu^2}} \leq \frac{1}{\left(\pi 2\nu^2\right)^{d/2}} e^{-\frac{\|U_j-B\|^2}{2\nu^2}}. \quad (72)
\]
The error probability for the case of decoding vector \(U_j = A\), is
\[
\Pr_e\left(\|\tilde{\delta}_j + \tilde{\Upsilon}_j\| > \|A + \tilde{\delta}_j + \tilde{\Upsilon}_j\|\right) = \Pr_e\left((A - B)^T \left(\tilde{\delta}_j + \tilde{\Upsilon}_j\right) < -\frac{A - B}{2}\right). \quad (73)
\]
For the case of correction of \(U_j = B\), the error probabilities are evaluated as
\[
\Pr_e\left(\|\tilde{\delta}_j + \tilde{\Upsilon}_j\| > \|B + \tilde{\delta}_j + \tilde{\Upsilon}_j\|\right) = \Pr_e\left((B - A)^T \left(\tilde{\delta}_j + \tilde{\Upsilon}_j\right) < -\frac{B - A}{2}\right). \quad (74)
\]
The decision regions can be separated into two hyperplanes \(H_1\) and \(H_2\) along \(B - A\), which separate \(U_j = A\) and \(U_j = B\). In other words, the correction-condition of a given noisy \(U_j\) is reduced to the following decision problem:
The correction of the noise of $\mathbf{U}_j'$ in the vector space $\mathbf{v}$ of $\mathbb{R}^d$ is depicted in Fig. 8.

Fig. 8. Alice’s error correction of the received noisy $\mathbf{U}_j'$ in the vector space $\mathbf{v}$ of $\mathbb{R}^d$. The scalars $A'$ and $B'$ refer to the values $A', B'$ of $\mathbf{U}_j'$. Alice divides the space into two hyperplanes $\mathcal{H}_1$ and $\mathcal{H}_2$, and classifies the received noisy $\mathbf{U}_j' \in \{A', B'\}$ into one of the hyperplanes.

As follows, by applying the procedure Alice can retrieve $\mathbf{U}_j \in \{A, B\}$ 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 $\Gamma^{d-1}$ 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 $\delta_j$ 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 $\delta_{j,i} = \frac{U_{j,i}}{C(X_{j,i})}C(\Delta_{j,i}) \in \mathbb{N}\left(0, \sigma_j^2\right)$, while on the sum of the noise of the $d$ units is a zero-mean Gaussian random variable $\sum_{i=0}^{d-1} \delta_{j,i} \in \mathbb{N}\left(0, \sigma_j^2\right)$, that is justified by the CLT and the Lyapunov-condition. Alice will correct the units in the following form:

$$U_j' = \sum_{i=0}^{d-1} U'_{j,i} = \frac{\sum_{i=0}^{d-1} C(X_{j,i})}{\sum_{i=0}^{d-1} C(X_{j,i})} \sum_{i=0}^{d-1} U_{j,i} = U_j + \delta_j \in \mathbb{R}. \quad (76)$$

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

$$\mathbf{U}_j = x(\mathbf{A} - \mathbf{B}) + \frac{1}{2}(\mathbf{A} + \mathbf{B}), \quad (77)$$

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:
\[ U'_j = x (A - B) + \frac{1}{2} (A + B) + \delta_j. \]  

From (78) follows that:

\[
U'_j = \sum_{i=0}^{d-1} \left( x (A_i - B_i) + \frac{1}{2} (A_i + B_i) + \delta_{j,i} \right) \\
= \sum_{i=0}^{d-1} x (A_i - B_i) + \frac{1}{2} \sum_{i=0}^{d-1} (A_i + B_i) + \delta_j \\
= \sum_{i=0}^{d-1} U'_{j,i} \\
= U_j + \frac{U_j}{C(X_j)} C(\Delta_j),
\]

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 (79), because she can apply a simpler process. For this purpose, she draws a new vector, \( d \):

\[
d = \frac{A - B}{\|A - B\|},
\]

where \( \|A - B\| = \sqrt{\sum_{i=0}^{d-1} (A_i - B_i)^2} \) is the effective distance of \( A \) and \( B \). A useful property of vector \( d \) drawn in (80), that any independent noise [15] (i.e., independent from the noise on \( U'_j \)) could live only in the orthogonal directions to \( d \), i.e., \( \{ n_1, \ldots, n_l \} \perp d \). It immediately follows, that the \( n_1, \ldots, n_l \) orthogonal directions will have no further importance for Alice in the decoding [15-19]. Since \( x \) is a scalar and in (78) the term \( \frac{1}{2} (A + B) \) is a constant, Alice introduces vector \( \chi \in v \) as follows:

\[
\chi \equiv U'_j - \frac{1}{2} (A + B) = x (A - B) + \delta_j.
\]

She also draws an orthogonal matrix \( M \), which contains \( d \) and the orthogonal directions \( n_1, \ldots, n_l \) with unit norm as:

\[
M = \begin{pmatrix}
  d \\
n_1 \\
n_2 \\
  \vdots \\
n_l
\end{pmatrix}.
\]

By multiplying \( M \) with \( \chi \) leads to:

\[
M\chi = \begin{pmatrix}
x \|A - B\| \\
0 \\
0 \\
0 \\
0
\end{pmatrix} + M\delta_j.
\]

From (83), it clearly follows that only \( x \|A - B\| \) and the first component of \( M\delta_j \) have relevance in the error-correction process, because all of the other components are orthogonal to \( d \) [15]. Since the evolution of \( d \) is a trivial process on Alice’s side, the received \( U'_j \) can be projected by
onto the direction of $d$, since all valuable information including the real noise is carried only by this direction. The projection $\mathcal{P}$ on $U'_j$ is made by $d^T \chi$, which then results in:

$$\mathcal{P}(U'_j) = d^T \chi$$

$$= \left( \frac{A-B}{|A-B|} \right)^T \left( x(A-B) + \delta_j \right)$$

$$= d^T (U'_j - \frac{1}{2} (A + B)).$$

(84)

The projected vector $\mathcal{P}(U'_j)$ 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. 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 the scalar space $\mathbb{R}$. As depicted in Fig. 9, the scalar reconciliation process does not require spherical rotations or any spherical operation, only standard operations.

As follows, only the first component of $M \delta_j$ has relevance in the error-correction, which in particular coincidences with the scalar quantity $\delta_j = \sum_{i=0}^{d-1} \delta_{j,i} = \frac{\sum_{i=0}^{d-1} C(\Delta_{j,i})}{\sum_{i=0}^{d-1} C(X_{j,i})} \sum_{i=0}^{d-1} U_{j,i}$ shown in (58). Putting the pieces together, $\mathcal{P}(U'_j)$ is evaluated as:

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

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

Proof.

Let $U_j \in \{a,b\} = \sum_{i=0}^{d-1} U_{j,i}$ from (79), $C(X_j) = \sum_{i=0}^{d-1} C(X_{j,i})$ 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:

$$\Pr(U_j = a \mid U'_j) \geq \Pr(U_j = b \mid U'_j).$$

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

$$\Pr(U_j = b \mid U'_j) \geq \Pr(U_j = a \mid U'_j).$$

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:

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

(89)

and:

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

(90)

which then leads to (for a comparison see (56) and (57)):

$$|U'_j - a| < |U'_j - b|$$

(91)

and:

$$|U'_j - a| > |U'_j - b|.$$  

(92)

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 $U_j = a$:

$$\Pr\left(U_j' = \frac{U_j}{\sqrt{C(X_j)}} C(\Delta_j) < \frac{\mu_a + \mu_b}{2} \mid U_j = a\right) = \Pr\left(U_j' = \frac{U_j}{\sqrt{C(X_j)}} C(\Delta_j) > \frac{\mu_a - \mu_b}{2}\right),$$

(93)

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

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

(94)

which clearly demonstrates that the error probability of scalar reconciliation exponentially converges to zero. As one can readily obtain from (94), for arbitrary large differences between $a$ and $b$, $Q\left(\frac{|a-b|}{2\eta}\right) \to 0$ [15-17].

Alice’s error-correction strategy is illustrated in Fig. 10. Alice chooses $a$ if $U'_j < \frac{\mu_a + \mu_b}{2}$, and selects $b$, if $U'_j > \frac{\mu_a + \mu_b}{2}$ holds.

![Fig. 10. Alice’s error correction in the scalar space. Alice corrects each $U'_j$ to rebuild the full key, $K$. The noise on a given $U'_j$ has variance $\eta^2$, which arises from the quantum channel. The Gaussian noise of the quantum-level transmission is survived on the raw-data level, and it has distorted Bob’s secret $U_j$ into $U'_j = U_j + \delta_j$ on Alice’s side.](image)

Thanks to the apparatus provided by maximum-likelihood decision theory and to the application of the Bayes’ rule [15-19], for a given $U_j$ one obtains error probability:

$$
\Pr\left(U'_j < \frac{\mu_a + \mu_b}{2} \mid U_j\right) = \Pr\left(\frac{|a-b|}{2\eta} < g\right)
= Q\left(\frac{|a-b|}{2\eta}\right)
= \Pr\left(error\right),
$$

(95)

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 Fig. 11.
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 Results

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 $\mathcal{N}$ of the Gaussian quantum channel is expressed as $\mathcal{N} = (\sigma^2_w - 1)(1 - T)T^{-1}$, where $T$ is the transmission, and $\sigma^2_w$ is the modulation variance [1] of the combined signal transmitted over $\mathcal{N}_2$, which has parameters that are accessible for the parties after a corresponding calibration phase prior to the start of the reconciliation process [1-4, 11]. The secret rate $R$ for the two-way CVQKD protocol, assuming homodyne measurements and RR, is

$$R = \frac{1}{2} \log \left( \frac{(1 - T + T^2)}{(1 - T)^2} \right) - H(\sigma^2_w) \ [1],$$

where $H$ is the Shannon entropy. Assuming reconciliation efficiency $0 \leq \beta \leq 1$, the key rate can be rewritten as

$$R = \beta I(A:B) - I(B:E),$$

where $I(B:E) < I(A:E)$. At a given SNR, the mutual information of Alice and Bob is

$$I(A:B) = \frac{1}{2} \log_2 \left( 1 + \text{SNR} \right) \ [1-8].$$

The SNR value can be determined as

$$\text{SNR} = \frac{\sigma^2_w}{\sigma^2_{N_2}},$$

where $\sigma^2_{N_2}$ is the variance of $\mathcal{N}_2$, which has parameters that can be calculated from $T$ and $\mathcal{N}$. In terms of $\beta$, the accuracy of the approximation of the Gaussian quantum channel can be expressed as $\beta I(A:B)$, which at low SNRs coincides with the approximation of a binary Gaussian channel.

In Fig. 12(a) 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

$$\lim_{N/d \to \infty} d \text{var} \left[ \delta_{0...N/d} \right] = \text{var} \left[ \delta_{0...N/d} \right] \approx \left( \sigma^2_{N_2} \right)_d$$

for arbitrary $d$ to maximize the SNR $= \sigma^2_w/\sigma^2_{\delta_j}$ of the converted logical channel. As depicted in Fig. 12(b), for $d \to \infty$, the efficiency converges to one, $\beta \to 1$, because the noise perfectly converges to a zero-mean Gaussian random variable.
Fig. 12. (a) The 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 PM-RR two-way CVQKD protocol, with homodyne measurements. The parameters are as follows. Excess noise $N = 0.015$, transmittance $T = 0.8$, variance $\sigma_\omega^2 = 1.06$, 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 $N_1$ and $N_2$, and the attacker model is equivalent to two independent Gaussian attacks applied separately on the two channels [7,8]).

In Fig. 13 the SNR of the logical binary Gaussian are depicted for various dimensions, at modulation variance $\sigma_\omega^2 = 1.06$ and variance $\sigma_{N_2}^2$ of the quantum channel.

Fig. 13. The SNRs of the logical channel at modulation variance $\sigma_\omega^2 = 1.06$. As the dimension increases the variance of the logical channel reaches the variance of the physical quantum channel. At $d = 16$ the variances perfectly coincide.
The performance of scalar reconciliation is summarized in Fig. 14. The performance of the analyzed protocol without scalar reconciliation with reconciliation efficiency $\beta = 0.9$, is depicted by the blue curve [7-8]. The scalar reconciliation at $d = 16$, improved the reconciliation efficiency to $\beta = 0.97$, which resulted in significantly higher transmission distances and secret key rates.

Fig. 14. The performance of scalar reconciliation in two-way PM-RR CVQKD at $d = 16$ (homodyne measurement at both sides). Excess noise: $\mathcal{N} = 0.015$, transmittance: $T = 0.8$, modulation variance: $\sigma_w^2 = 1.06$, channel correlation: $n_c = 0.5$.

The scalar reconciliation applied on the analyzed two-way CVQKD protocol resulted in approximately 160 km of achievable transmission distance. 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 two-way CVQKD can significantly be improved because at low SNRs the capacity of the logical binary Gaussian channel coincides with the capacity of the Gaussian quantum channel, and the logical channel resulted from the conversion can approximate it with arbitrary-high precision.

6 Conclusions

The continuous-variable QKD systems have a great advantage over the DVQKD protocols that can be established over the current telecommunication networks and require only standard network components and devices. The one-way CVQKD protocols have almost reached their physical limits, and no further exploitable resources remain to significantly improve the key rates and transmission distances. The two-way CVQKD protocols are equipped with much stronger hardware in comparison to the one-way protocols, however the lack of the efficient post-processing, up
to this point, made it not possible to exploit the real potential of the protocol. 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 CVQKD scenario, moreover it has strict limitations on the available dimensions. The proposed scalar reconciliation eliminates the use of multidimensional spherical space along with the dimensional boundaries and can be used in arbitrary high dimensions. The scalar reconciliation process neither requires any physical-layer tomography [1-8], and only standard operations and calculations needed in the level of raw data. The method provides unconditional security, and allows a much easier 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 two-way CVQKD.

Acknowledgements
The author would like to thank Professor Sandor Imre for useful discussions. The results are supported by the grant COST Action MP1006.

References
[1] S. Pirandola, S. Mancini, S. Lloyd and S. L. Braunstein. Nature Phys. 4 726, (2008).
[2] S. Pirandola, R. Garcia-Patron, S. L. Braunstein and S. Lloyd. Phys. Rev. Lett. 102 050503. (2009)
[3] S. Pirandola, A. Serafini and S. Lloyd. Phys. Rev. A 79 052327. (2009).
[4] S. Pirandola, S. L. Braunstein and S. Lloyd. Phys. Rev. Lett. 101 200504 (2008).
[5] C. Weedbrook, S. Pirandola, S. Lloyd and T. Ralph. Phys. Rev. Lett. 105 110501 (2010).
[6] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. Ralph, J. Shapiro, and S. Lloyd. Rev. Mod. Phys. 84, 621 (2012).
[7] M. Sun, X. Peng, Y. Shen, H. Guo. Int. J. Quant. Inf. 10 1250059 (2012)
[8] M. Sun, Xiang Peng and Hong Guo. J. Phys. B: At. Mol. Opt. Phys. 46 085501 (2013)
[9] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A 84, 062317 (2011).
[10] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Phys. Rev. A 86, 032309 (2012).
[11] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier, Phys. Rev. A 77, 042325 (2008).
[12] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, arXiv:1210.6216v1 (2012).
[13] A. Leverrier, R. Garcia-Patron, R. Renner, and N. J. Cerf, Arxiv preprint arXiv:1208.4920 (2012).
[14] S. Imre and L. Gyongyosi. Advanced Quantum Communications - An Engineering Approach. Wiley-IEEE Press (New Jersey, USA), (2012).
[15] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*, Cambridge University Press, (2005).

[16] J. Hamkins and K. Zeger. Asymptotically efficient spherical codes—Part I: Wrapped spherical codes, *IEEE Trans. Inform. Theory*, vol. 43, pp. 1774–1785, (1997).

[17] P. F. Swaszek and J. B. Thomas. Multidimensional spherical coordinates quantization, *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 570–576, (1983).

[18] K. Miller. *Multidimensional Gaussian Distributions*. New York: Wiley, (1964).

[19] J. Hamkins. *Design and analysis of spherical codes*, Ph.D. dissertation, Univ. Illinois at Urbana-Champaign, (1996).

[20] J. H. Conway and D. A. Smith, *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*, A K Peters/CRC Press, (2003).

[21] T. Richardson and R. Urbanke, *Modern Coding Theory*, (Cambridge University Press, New York, NY, USA), (2008).

[22] A. Gersho. Asymptotically optimal block quantization, *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 373–380, (1979).

[23] D. J. Sakrison. A geometric treatment of the source encoding of a Gaussian random variable, *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 481–486, (1968).

[24] J. Hamkins and K. Zeger. Gaussian Source Coding With Spherical Codes, *IEEE Trans. Inform. Theory*, vol. 48, no 11, (2002).

[25] L. Hanzo, H. Haas, S. Imre, D. O’Brien, M. Rupp, L. Gyongyosi. Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless, *Proceedings of the IEEE*, Volume: 100, Issue: Special Centennial Issue, pp. 1853-1888. (2012).

[26] J. Rice. *Mathematical Statistics and Data Analysis* (Second ed.), Duxbury Press, ISBN 0-534-20934-3 (1995).
## Supplemental Information

### S.1 Notations

The notations of the manuscript are summarized in Table S.1.

**Table S.1.** The summary of the notations used in the manuscript.

| Notation                                                                 | Description                                                                                                                                 |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| $|\varphi_i⟩ = |x_{A,i} + x'_{B,i} + i(p_{A,i} + p'_{B,i})⟩$                           | The first mode of the combined beam, phase space vector, where $x_{A,i}, x'_{B,i}$ and $p_{A,i}, p'_{B,i}$ are the position and momentum quadratures. |
| $|φ_i⟩ = |x_{A,i} - x'_{B,i} + i(p_{A,i} - p'_{B,i})⟩$                           | The second mode of the combined beam, phase space vector, transmitted to Bob, where $x_{A,i}, x'_{B,i}$ and $p_{A,i}, p'_{B,i}$ are the position and momentum quadratures. |
| $|ξ_i⟩ = |x'_{A,i} - x''_{B,i} + i(p'_{A,i} - p''_{B,i})⟩$                       | The noisy version of phase space state $|φ_i⟩$, with the noisy quadratures.                                                                 |
| $X$                                                                     | Alice’s $N$-unit length raw data generated by $N$ random quadrature measurements. Binary string, consists of $N/d$ number of $d$-dimensional Gaussian random vectors $X_j ∈ \mathbb{R}^d$. |
| $X'$                                                                    | Bob’s $N$-unit length raw data generated by $N$ random quadrature measurements. Binary string, consists of $N/d$ number of noisy $d$-dimensional Gaussian random vectors $X'_j ∈ \mathbb{R}^d$. |
| $X_i = x_{A,i} + x'_{B,i}$; $X_i = p_{A,i} + p'_{B,i}$                 | Alice’s raw data unit, obtained from a random quadrature measurement, where $x_{A,i}, x'_{B,i}$ and $p_{A,i}, p'_{B,i}$ are the position and momentum quadratures. |
| $X'_i = x'_{A,i} + x''_{B,i}$; $X'_i = p'_{A,i} + p''_{B,i}$            | Bob’s noisy raw data unit, obtained from a random quadrature measurement and by a correction $+2p_{B,i}$ or $+2p'_{B,i}$, while $x'_{A,i}, x''_{B,i}$ and $p'_{A,i}, p''_{B,i}$ are the noisy position and momentum quadratures. |
| $X_j ∈ \mathbb{R}^d : \{X_{j,0}, X_{j,1},..., X_{j,d-1}\}$              | Alice’s $d$-dimensional Gaussian random vector ($d$ unit length Gaussian random vector), where $X_{j,i}$ is a Gaussian random variable. |
| $X_{j,i} ∈ \mathbb{R}$, $X'_{j,i} ∈ \mathbb{R}$                        | The $i$-th unit of $j$-th vector $X_j$ and $X'_j$.                                                                                       |
| $X'_j ∈ \mathbb{R}^d : \{X'_{j,0}, X'_{j,1},..., X'_{j,d-1}\}$         | Bob’s noisy $d$-dimensional Gaussian random vector ($d$ unit length vector), where $X'_{j,i} = x'_{A,i} + x''_{B,i}$ or $X'_{j,i} = p'_{A,i} + p''_{B,i}$ is a |
Gaussian random units obtained from a quadrature measurement.

$K = \left\{ U_0, \ldots, U_{(N/d)-1} \right\} \in \mathbb{R}^{N/d}$,

$U_j = \left\{ U_{j,0}, U_{j,1}, \ldots, U_{j,d-1} \right\} \in \mathbb{R}^d$,

$U_j \in \{a,b\} \subset \mathbb{R}$

Bob’s secret key vector. The full key is granulated into $N/d$ number of $U_j \in \mathbb{R}^d$ vectors.

$x_j'U_j \in \mathbb{R}^d$

Bob’s $d$-dimensional vector sent to the classical channel.

$x_{j,i}'U_{j,i} \in \mathbb{R}$

A unit of Bob’s $d$-dimensional message sent to the classical channel.

$C(\cdot)$

The Gaussian CDF function.

$\mathfrak{C}(\cdot)$

Covariance matrix.

$D_d(\cdot)$

Dirac distribution of a $d$-dimensional vector.

$L$

Lyapunov coefficient, $L > 0$.

$U_j' = \sum_{i=0}^{d-1} U_{j,i}'$

The noisy version of Bob’s secret $U_j$, and its unit $U_{j,i}$.

$x_{j,i}'(\cdot) = \left( C(x_{j,i}')U_{j,i} \right) / C(x_{j,i})$

$x_{j,i}' \in \mathbb{R}$

$x_{j,i}' = 1 / C(x_{j,i})$

The noisy version of Bob’s secret $U_j$, and its unit $U_{j,i}$.

$\delta_{j,i}$

Noise on $U_j' = \sum_{i=0}^{d-1} U_{j,i}'$, and on unit $U_{j,i}$.

$\eta = \left( \sigma_{\delta_j}^2 \right)^{1/2}$

Standard deviation of the noise vector $\vec{\delta}_j$.

$\Lambda_j = \mathbb{N}(0,1)_d \in \mathbb{R}^d$,

$\Lambda_{j,i} = \mathbb{N}(0,1) \in \mathbb{R}$

Standard Gaussian random noise vector, and the noise of the $i$-th unit of the $j$-th block $X_{j,i}$.

$\Delta_j = \mathbb{N}(0,\sigma_2^2)_d \in \mathbb{R}^d$

Gaussian random noise vector of the quantum channel $\mathcal{N}_2$ on $X_j$.

$\Delta_{j,i} = \mathbb{N}(0,\sigma_2^2) \in \mathbb{R}$

The $i$-th unit of $j$-th noise vector, that results raw data unit $X_{j,i}' = X_{j,i} + \Delta_{j,i}$.

### S.2 Abbreviations

**AWGN**  Additive White Gaussian Noise

**BAWGN**  Binary Additive White Gaussian Noise

**BS**  Beam Splitter

**BSC**  Binary Symmetric Channel

**CDF**  Cumulative Distribution Function

**CLT**  Central Limit Theorem

**CV**  Continuous-Variable

**DV**  Discrete-Variable

**LDPC**  Low Density Parity Check

**PM**  Prepare-and-Measure: entanglement-free protocol

**RR**  Reverse Reconciliation

**SNR**  Signal-to-Noise Ratio
S.3 Numerical Evidence I. 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 \( \sigma^2_{X} = 100 \). In Fig. S.1(a) the distribution of the \( X_{j,i} \) Gaussian random raw data units is shown. Fig. S.1(b) 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.

The distribution of the Gaussian noise vector \( \Delta_{j,i} \in \mathcal{N}(0, \sigma^2_{\mathcal{N}_2}) \) of the quantum channel \( \mathcal{N}_2 \), at \( \sigma^2_{\mathcal{N}_2} = 4 \) is shown in Fig. S.2.

Fig. S.1. (a) The distribution of Alice’s raw data units. The units follow Gaussian random distribution. (b) The distribution of the CDF-transformed units. The probability distribution has changed into uniform in the range of \([0,1]\).

Fig. S.2. 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 $C(X'_{j,i})$ units have a modified distribution with variance $\sigma^2 = \sigma^2_X + \sigma^2_{X_2} = 104$, as depicted in Fig. S.3. The Gaussian noise on the units is added by $\Delta_{j,i} \in \mathbb{N}(0, \sigma^2_{X_2})$.

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

**S.4 Numerical Evidence II. Noise on the random secret**

This example demonstrates that the noise $\delta_j = \frac{\sum_{i=0}^{d-1} C(\Delta_{j,i})}{\sum_{i=0}^{d-1} C(X_{j,i})} \sum_{i=0}^{d-1} U_{j,i}$ 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 the noise of the logical binary channel can be approximated by a Gaussian random variable $\delta_j = \sum_{i=0}^{d-1} \delta_{j,i} \in \mathbb{N}(0, \sigma^2_{\delta_j})$.

Let $N = 1000$ units, the amount of sample raw data units $X_{j,i}$, $X'_{j,i}$. The quantity $C(\Delta_j) = C(X'_j) - C(X_j)$ measures the difference of $C(X'_j)$ and $C(X_j)$, i.e., the noise of Bob’s CDF-transformed data. Let $X_j \in \mathbb{N}(0, \sigma^2_X = 100)$ and $X'_j \in \mathbb{N}(0, \sigma^2_{X'} = 104)$. The example uses an $d = 16$ dimensional approximation. The distribution of the error $C(\Delta_{j,i})$ of the CDF-transformed raw data units $C(X'_{j,i})$, $C(X_{j,i})$ are depicted in Fig. S.4.
Fig. S.4. The distribution of the error \( C(\Delta_{j,i}) = C(X'_{j,i}) - C(X_{j,i}) \) on the CDF-transformed raw data units.

In Fig. S.5(a) the ratio \( C(X'_{j,i})/C(X_{j,i}) \) of the CDF-transformed units is shown in Fig. S.5(a). In the ideal (noise-free) case the ratio equals to 1. In Fig. S.5(b) the distribution of the quantity \( C(\Delta_{j,i})/C(X_{j,i}) \) is shown.

Fig. S.5. (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 \( C(\Delta_{j,i})/C(X_{j,i}) \).

In Fig. S.6(a) 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 Fig. S.6(b) the distribution of \( \delta_j \) on \( U'_j \), using \( U_j = \sum_{i=0}^{d-1} U_{j,i} \in \{-400, -400\} \) is depicted.

The distribution of \( \delta_j \) is given by the formula of \( \mathcal{N}(0, \sigma^2_{\delta_j}) \), and the approximation of the binary Gaussian logical channel is justified by the CLT and the Lyapunov-condition.
Fig. S.6. (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 $\mathbb{N}\left(0, \sigma_{\delta_j}^2\right)$.

S.5 Preliminaries

Spherical Code

A $d$-dimensional spherical code $\mathcal{X}$ is defined over the $d$-dimensional unit sphere $\Gamma^{d-1}$, given by $\Gamma^{d-1} = \{x = (x_0, x_1, \ldots, x_{d-1}) \in \mathbb{R}^d : \|x\| = 1\}$, and $\|x\| = 1$ is the unit norm. The $(d - 1)$-dimensional surface $S(\Gamma^{d-1})$ of $\Gamma^{d-1}$ is defined as $S(\Gamma^{d-1}) = 2\pi^{d/2}/\mathcal{G}(d/2)$, where $\mathcal{G}(d/2) = \int_0^{\infty} t^{(d/2)-1} e^{-t} dt$ is the gamma function [24]. The number of codewords of the code is $|\mathcal{X}|$, the smallest dimension $d_{\min}$ of any Euclidean space for the spherical code $\mathcal{X}$ is $d_{\min} = \dim|\mathcal{X}|$, while the minimum distance between any two elements $x$ and $y$ of $\mathcal{X} \subseteq \Gamma^{d-1}$, $x \neq y$, is $D = \min\left\{\|x - y\|^2\right\}$.

Gaussian Random Spherical Vectors

Let $\mathbf{x} = \left(X_0, \ldots, X_{d-1}\right)^T \in \mathbb{R}^d$ be a Gaussian random vector with independent components, and with norm $\|\mathbf{x}\|$ drawn from an $\mathbb{N}\left(0, \sigma^2\right)$ memoryless Gaussian source. Over the $d$-dimensional
unit sphere $\Gamma^{d-1}$, spherical Gaussian random vector $E[\|X\|\|X\|/\|X\|] \in \Gamma^{d-1} \in \mathbb{R}^d$ has radius $r = E\|X\|$, where $E$ is the mean of the norm $\|X\|$, defined [24] as

$$E[\|X\|] = \frac{\sqrt{2\sigma^2 \beta(\frac{1}{2})}}{\beta(\frac{1}{2}, \frac{1}{2})} = \frac{\sqrt{2\sigma^2 \beta(\frac{1}{2}, \frac{1}{2})}}{\beta(\frac{1}{2}, \frac{1}{2})},$$

(S.1)

where $\beta(x, y) = \frac{\beta(x) \beta(y)}{\beta(x + y)}$, is the beta function, while $E[\|X\|^2] = d\sigma^2$. The Gaussian random vector $X \in \mathbb{R}^d$ over $\Gamma^{d-1}$ has a probability density function

$$f(X) = \frac{2^{d-1}}{\beta(d/2\sigma^2)} \frac{e^{-\frac{1}{2} \|X\|^2}}{\sigma^d \Gamma(d/2)},$$

(S.2)

and variance

$$\text{var}[X] = d\sigma^2 - \frac{2\sigma^2}{\beta(d/2\sigma^2)}. \quad \text{(S.3)}$$

For $d \to \infty$, $E\|X/\sqrt{d\sigma^2}\| \to 1$, and $r = \lim_{d \to \infty} \|X/\sqrt{d\sigma^2}\| \to 1$. The distribution of $r$ approximates the Dirac distribution $\mathcal{D}_d(x)$, and gets to arbitrary close for $d \to \infty$. 

42